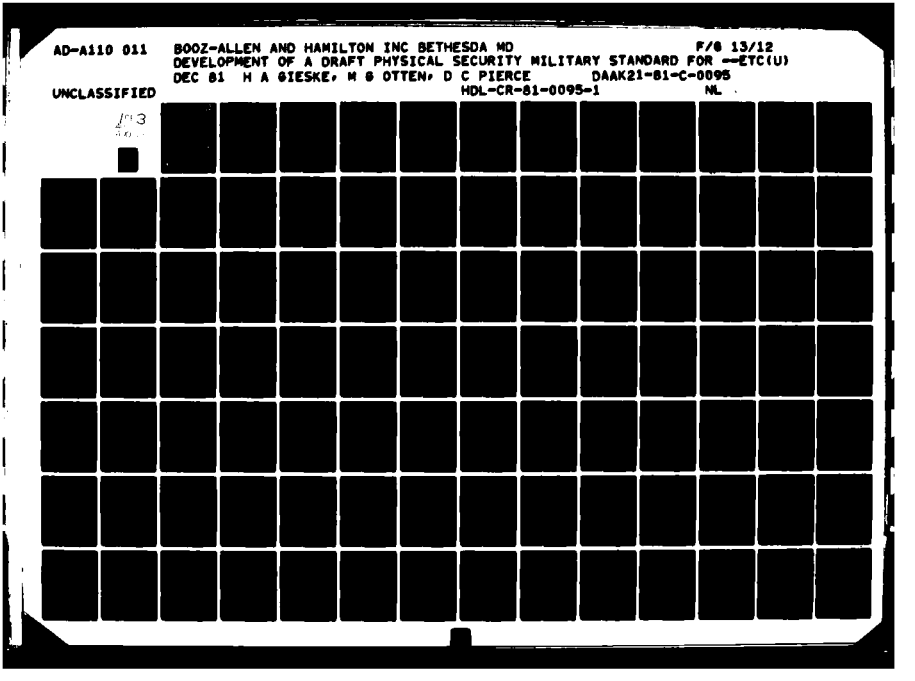
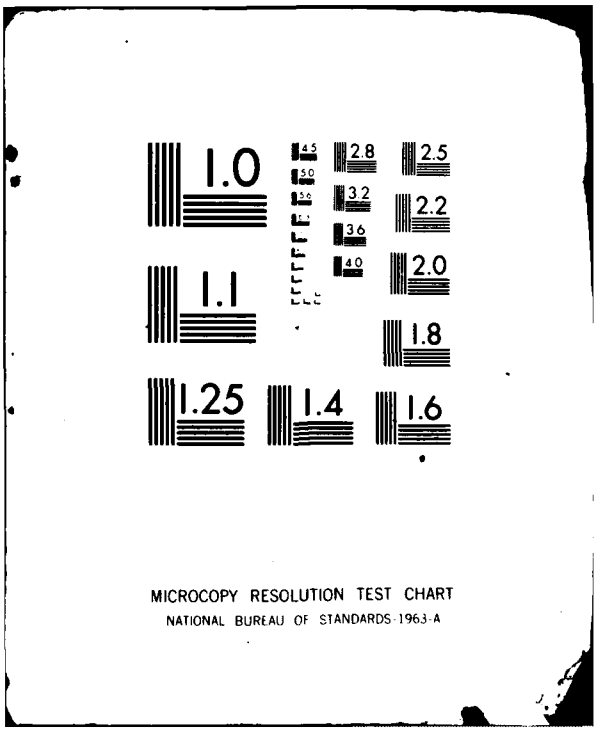

AD-A110 011
BOOZ-ALLEN AND HAMILTON INC BETHESDA MD
F/G 13/12
DEVELOPMENT OF A DRAFT PHYSICAL SECURITY MILITARY STANDARD FOR --ETC(U)
DEC 81 H A GIESKE, M G OTTEN, D C PIERCE
DAAK21-81-C-0095
UNCLASSIFIED
HDL-CR-81-0095-1
NL


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

LEVEL II

12

HDL-CR- 81-0095-1

December 1981

DEVELOPMENT OF A DRAFT PHYSICAL SECURITY MILITARY STANDARD FOR DEFENSE COMMUNICATIONS SYSTEM FACILITIES

by Harry A. Gieske
Michael G. Otten
Donald G. Pierce
Donald R. Richards
Jennie Stevens
Robert L. Kitzmiller

Prepared by
Booz, Allen & Hamilton Inc.
4330 East West Highway
Bethesda, Md 20814

Under contract
DAAK21-81-C-0095

U.S. Army Electronics Research and Development Command
Harry Diamond Laboratories
Adelphi, MD 20783

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER HDL-CR-81-0095-1	2. GOVT ACCESSION NO. AD-A110011	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) DEVELOPMENT OF A DRAFT PHYSICAL SECURITY MILITARY STANDARD FOR DEFENSE COMMUNICATIONS SYSTEM FACILITIES		5. TYPE OF REPORT & PERIOD COVERED Final Report 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Harry A. Gieske, Michael G. Otten, Donald C. Pierce, Donald R. Richards, Jennie Stevens, Robert L. Kitzmiller		8. CONTRACT OR GRANT NUMBER(s) DAAK21-81-C-0095
9. PERFORMING ORGANIZATION NAME AND ADDRESS Booz, Allen & Hamilton Inc. 4330 East West Highway Bethesda, Maryland 20814		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Prog. El 33126K MIPR HC1001040055
11. CONTROLLING OFFICE NAME AND ADDRESS Harry Diamond Laboratories [illegible] Hill Road [illegible]783		12. REPORT DATE [illegible]82 13. NUMBER OF PAGES Contract Monitor, Robert V. Garver
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) 15a. DECLASSIFICATION/ DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

HDL Project E040E1
PRON: WSO-10401NSA9

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Physical Security	Threat Analysis
Sensors	Protection Allocation
Fences	Threat Vulnerability Matrix
Barriers	Protection Allocation Matrix
Security Zones	Security Program Planning

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

A comprehensive draft military standard for the physical security of Defense Communication System facilities was developed. The resulting military standard provides instructions and specifications for performing threat analysis, vulnerability analyses, protection allocations, security measure implementation and security system testing. The standard provides comprehensive guidelines and procedures for use by site operators or security system planners so that the unique security requirements of both manned and unmanned communication facilities are met. (over)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

The detailed technical requirements of thirty different security measures and devices are given as unit page type standards. These unit page standards have been tailored to the specific and sometimes unique security situations found at Defense Communication System sites.

This report describes the overall effort in developing the draft standard while the draft military standard itself is contained in Apendix A.

CONTENTS

APPENDIX A

DRAFT OF MILITARY STANDARD FOR THE PHYSICAL SECURITY OF DCS FACILITIES

1. INTRODUCTION

1.1 Background

Over the past several years, the Defense Communications Agency (DCA) has been addressing the vulnerability of Defense Communications System (DCS) assets to a variety of threats. Among the vulnerabilities being addressed are those of sabotage and physical damage of communication sites by individuals and groups who may be characterized as vandals, terrorists, foreign agents and special operations forces.

Under DCA sponsorship the vulnerabilities of existing DCS facilities were identified in programs accomplished by the Harry Diamond Laboratories, Department of the Army.[1,2,3,4] Subsequently, the Defense Communications Agency prepared a circular dealing with various aspects of the physical security of DCS facilities.[5]

Although the previous work had identified susceptibilities and potential countermeasures, it became apparent that a need existed for a comprehensive standard by which DCS facility operators and users could systematically and uniformly plan and conduct a physical security program. Such a security program must meet the requirements for protecting both manned and unmanned facilities. Recognition of this need led DCA to the preparation of a draft physical security standard. The development of this draft standard was the primary objective of the work described in this report.

This report is divided into two volumes. The first volume provides an overview of the effort and the rationale for the contents and the format of the resulting draft military standard. The second volume is the draft "Military Standard for the Physical Security of DCS Facilities."

---

[1]Harry A. Gieske et al., Impact of Sabotage on Defense Communications System Facilities: Phase I (U), Harry Diamond Laboratories TM-76-34 (December 1976). (Confidential)

[2]Murry B. Ginsberg et al., Impact of Sabotage on DCS Facilities: Phase II, Harry Diamond Laboratories TM-77-19 (October 1977).

[3]Murry B. Ginsberg at al., Impact of Sabotage on Manned DCS Facilities: Task I (U), Harry Diamond Laboratories TM-78-1 (November 1978). (Secret)

[4]Murry B. Ginsberg, Impact of Sabotage on Manned DCS Facilities: Task II, Harry Diamond Laboratories TM-78-13 (November 1978).

[5]Defense Communications Agency, Physical Countermeasures for DCS Facilities (Draft), DCA Circular 310-90-1.

1.2 Scope of Effort

The primary objective of this effort was the development of a comprehensive draft standard for the physical security of DCS facilities. However, various intermediate objectives had to be achieved to assure consistency and compatibility of the resulting standard with Department of Defense and service policies and standards relating to security programs and equipment. Compatibility was also required with survivability measures proposed for dealing with the high altitude electromagnetic pulse threat, to which DCS facilities may also be exposed.

As a result of the need for a comprehensive and compatible standard, the following intermediate tasks were defined:

1. Review and analysis of potential physical security threats ranging from vandals to trained special operations forces;

2. Collection and analysis of existing service security practices and standards;

3. Identification and assessment of the applicability of existing and developmental security system equipments;

4. Synthesis of security measures tailored to the special requirements of DCS facilities.

Work conducted to accomplish some of these intermediate objectives has been reported in companion reports.[6,7,8]

2. SYNTHESIS OF MILITARY STANDARD FOR PHYSICAL SECURITY

2.1 Guidelines for Synthesis of the Standard

For the preparation of the military standard several guidelines were given which directed the content and format of the resulting standard. Among the guidelines influencing the synthesis of the standard are those discussed below.

---

[6]Threat Delineation for DCS Phusical Security (U), Booz, Allen & Hamilton Inc., (March 1981). (Secret)

[7]"Development of Security Measures: Implementation Instructions for MIL-STD on Physical Security for DCS Facilities," (U), HDL-CR-81-024-1, Booz, Allen & Hamilton Inc., (July 1981). (Unclassified)

[8]"Development of Threat Vulnerability Matrix for DCS Facilities," (U), HDL-CR-81-0025-1, Booz, Allen & Hamilton Inc., (October 1981). (Unclassified)

1. The resulting document was to be consistent, as much as possible, with the requirements of MIL-STD-962,[9] which provides the specifications and format for writing military standards. This consistency requirement led to the content of specific chapters and to the differentiation between "required" practices and "permissible" practices for providing security measures at DCS facilities.

2. It was anticipated that the resulting military standard would be subject to changes as new developments occurred in security system equipment. Therefore, requirements dealing with the installation and testing of equipment were put in the form of unit pages which could be revised and inserted in the military standard without disturbing the integrity of the overall standards.

3. The resulting military standard was to be consistent with the design philosophy reflected in work done by DCA in connection with the protection of DCS facilities against high altitude electromagnetic pulse effects.[10] This guideline did not perturb the overall effort in the physical security standard preparation since the concept of zonal or layered protection is entirely consistent with physical security system design.

2.2 Special Considerations in Standard Development

In planning and preparing the content of the military standard for physical security of DCS sites, several special considerations had to be borne in mind. These considerations included:

1. The DCS consists of both manned and unmanned facilities.

2. While the general nature and function of DCS facilities are similar throughout the system, a wide variety of factors influenced the appropriateness and allowability of various security measures. These factors include host nation agreements, terrain, and the availability of responsive security forces.

3. Security programs must often be planned and executed by personnel not trained as security specialists.

4. Not all DCS facilities warrant the same degree or level of security investment.

---

[9]"Military Standard, Outline of Forms and Instructions for the Preparation of Military Standards and Military Handbooks," MIL-STD-962, Department of Defense, (September 1975).

[10]DSN Design Practices for High Altitude Electromagnetic PUlse (HEMP) Protection, Draft A, (30 May 1980), Harry Diamond Laboratories, Adelphi, Maryland.

5. Implementation of security measures often will be budgeted over several years.

6. While new DCS facilities will be constructed from time to time, and may include security measure implementation during initial construction, most security measures will be implemented at existing facilities.

All of these considerations were taken into account as security measures were proposed, analyzed, rejected, and/or adopted for use in the standard.

2.3 Work Breakout and Phasing

The work associated with the development of the draft military standard was divided into five subtasks. These subtasks were: 1) preparation of a preliminary draft of the desired military standard; 2) collection of additional security measures information and the generation of security measures concepts; 3) review of site survey information; 4) review and analysis of agency comments on the preliminary draft; and 5) preparation of a revised draft standard.

The first subtask was completed in an intensive, first phase effort. This effort resulted in an initial version of the military standard which was circulated to various DOD agencies and the services for comment and critique. This initial version was not complete and lacked specific security measures associated with unique sites. The emphasis in the first phase effort was on the security of generic sites, and the policies and procedures applicable thereto.

While agency comments were being formulated, work was performed on the second and third subtasks. Information was collected on existing and developmental security equipment. Contacts were made with the Army Project Office for Physical Security Equipment to ascertain security equipment developments applicable to DCS sites. Vendor data on security equipment were collected and organized into a reference file.

In a parallel activity, the Harry Diamond Laboratories undertook a survey of all DCS sites to identify site factors which would have impact upon the implementation of security measures. As part of the military standard development effort, the returned survey questionnaires were reviewed and analyzed. From this activity the characteristics of generic and unique sites were derived.

The final phase of the military standard development effort commenced with the receipt of agency comments on the first version of the standard. A thorough review and redrafting of the document was completed to include: (1) the agency comments and concerns dealing with requirements, procedures, and impact of the standard; (2) utilization of the survey information, particularly that information pertaining to the characteristics of unique sites; (3) specific security measures for use at

unique sites; and (4) development of security test procedures and their inclusion in the standard or unit pages.

3. RESULTS

3.1 Structure of the Draft Military Standard for Physical Security

The structure of the resulting military standard was devised to permit the application of "defense-in-depth" concepts to the planning and execution of security programs for DCS sites. The defense-in-depth concept was implemented through the use of five security zones or layers of protection. Each security zone has an objective or primary purpose. These are enumerated below:

Zone	Purpose
0	Deterrence
1	Detection
2	Alarm assessment
3	Assessment and delay
4	Delay and dapture (or denial)

The main body of the military standard is topically organized in relation to the five zones. Security measures appropriate to a specific zone are grouped in one section. In similar fashion, threat analysis and protection allocations are keyed to the use of the five security zones.

With the structure of the main body (that is, Section 5) of the draft standard organized along the use of five zones, the rest of the standard is organized according to the requirements of MIL-STD-962. MIL-STD-962 provides options in the preparation of military standards. One option is appropriate for a military standard covering many pages. Another option, called "unit pages," is appropriate for a one-page standard. The Draft Military Standard for Physical Security of DCS Sites combines both types of military standard formats. The multipage format is used for sections of the standard expected to remain stable over a period of time, while the unit page format is used to present requirements on equipment and test procedures likely to change as developments occur in security equipment.

3.2 Characteristics of Unique Sites

Before work on this standard was begun, it was recognized that not all DCS sites could be treated identically. While DCS sites have a similar mission, and often similar equipment, local conditions often make the security situation unique, thus prohibiting the implementation of generic security measures. Therefore, it was determined that the military standard would require a section dealing with unique sites.

The site survey data analysis showed that there are five aspects which may make a DCS site unique in the implementation of security measures. These aspects are:

- Site size
- Colocation with other activities
- Proximity to uncontrollable terrain or space
- Soil conditions
- Unique site components

Site size renders a site unique if the site is so small that a multiple zone approach to deterrence, detection, and delay is not feasible, or if the site is so large that incorporation of the whole site in a multiple zone defense is impractical operationally or is too costly.

Colocation with other activities renders a site unique if the responsibility for security within the site becomes ambiguous or impossible to enforce in areas required for adequate security measures. This may be the case when site users include commercial users or foreign nationals.

Proximity to uncontrollable terrain occurs when the site's critical assets are adjacent to public access thoroughfares, other buildings, or terrain. DCS facilities located in buildings contiguous to walkways and highways often leave no barrier, except a single wall, between critical assets and a potential adversary. As a site qualification factor, proximity to uncontrollable terrain is often combined with site size, resulting in a severely limited set of applicable physical security measures.

Soil conditions may make the installation of sensors difficult or impractical, or may limit the kinds of construction feasible on a given site. Permafrost areas or marsh areas could limit fence line or wall construction and sensor emplacement.

Unique site equipment may render a site unique when critical site components cannot be protected by the security measures identified in the standard. At the time this report was written, no such unique site equipment was identified.

The characteristics of unique sites formed the basis of the security measures contained in section 5.2.4 of the military standard.

4. CONCLUSIONS

The physical security of the diverse communication sites of the DCS requires a combination of measures. Ideally, these measures provide the effects of: (1) deterrence, (2) detection, (3) alarm assessment, (4) intrusion delay, and (5) intruder capture. A draft military standard has been developed for the physical security of DCS sites. This standard prescribes a systematic approach for planning and specifying security programs which accomplish all five effects.

The draft standard for physical security has been developed utilizing the principle of preparing a defense in depth against an attacking force. The standard applies this principle to generic sites and presents the user with a methodology for achieving a defense in depth through the use of five security zones, each of which provides increasing levels of security measure effectiveness.

The draft military standard presents a comprehensive prescription for the process of threat analysis, site vulnerability analysis, and the specification of appropriate security measures. The draft military standard is thus a suitable basis for the initial design of security measures at a new facility or for upgrading the security at existing facilities.

In preparing the draft military standard, effort was made to assure the usefulness of the standard to personnel not trained as security specialists. Thus the standard may be used by site operating personnel, command security specialists, or facility planners.

LITERATURE CITED

1. Harry A. Gieske et al., Impact of Sabotage on Defense Communications System Facilities: Phase I (U), Harry Diamond Laboratories TM-76-34 (December 1976). (Confidential)

2. Murry B. Ginsberg et al., Impact of Sabotage on DCS Facilities: Phase II, Harry Diamond Laboratories TM-77-19 (October 1977).

3. Murry B. Ginsberg at al., Impact of Sabotage on Manned DCS Facilities: Task I (U), Harry Diamond Laboratories TM-78-1 (November 1978). (Secret)

4. Murry B. Ginsberg, Impact of Sabotage on Manned DCS Facilities: Task II, Harry Diamond Laboratories TM-78-13 (November 1978).

5. Defense Communications Agency, Physical Countermeasures for DCS Facilities (Draft), DCA Circular 310-90-1.

6. Threat Delineation for DCS Phusical Security (U), Booz, Allen & Hamilton Inc., (March 1981). (Secret)

7. "Development of Security Measures: Implementation Instructions for MIL-STD on Physical Security for DCS Facilities," (U), HDL-CR-81-024-1, Booz, Allen & Hamilton Inc., (July 1981). (Unclassified)

8. "Development of Threat Vulnerability Matrix for DCS Facilities," (U), HDL-CR-81-0025-1, Booz, Allen & Hamilton Inc., (October 1981). (Unclassified)

9. "Military Standard, Outline of Forms and Instructions for the Preparation of Military Standards and Military Handbooks," MIL-STD-962, Department of Defense, (September 1975).

10. DSN Design Practices for High Altitude Electromagnetic PUlse (HEMP) Protection, Draft A, (30 May 1980), Harry Diamond Laboratories, Adelphi, Maryland.

DISTRIBUTION LIST:

Administrator
Defense Technical Information Center
Attn: DTIC-DDA (12 copies)
Cameron Station, Building 5
Alexandria, VA 22314

Harry Diamond Laboratories
Attn: CO/TD/TSO/Division Directors
Attn: Record Copy, 81200
Attn: HDL Library, 81100 (2 copies)
Attn: HDL Library, 81100 (Woodbridge)
Attn: Technical Reports Branch, 81300
Attn: Chairman, Editorial Committee
Attn: Legal Office, 97000
Attn: Chief, 20240
Attn: R. Garver, 21100 (5 copies)

DRAFT

MILITARY STANDARD FOR THE PHYSICAL SECURITY OF DCS FACILITIES

30 OCTOBER 1981

Prepared for

Defense Communications Engineering Center
ATTN: Code R-810/J. Worthington
1860 Wiehle Ave.
Reston, VA 22090
Under MIPR #HCC1001-0-40055, Task No. 11720501

Prepared by

Booz, Allen, & Hamilton Inc.
4330 East West Highway
Bethesda, MD 20814

Under Contract DAAK 21-81-0095
U.S. Army Electronics R&D Command
Harry Diamond Labs
2800 Powder Mill Rd.
Adelphi, MD 20783

APPENDIX A

TABLE OF CONTENTS

L I S T O F F I G U R E S

LIST OF TABLES

1. SCOPE

1.1 General. This standard establishes the procedures and practices in planning, implementing and testing of physical security programs for the protection of sites and associated facilities serving the Defense Communications System (DCS).

1.2 Application. This standard applies to all government owned, operated and maintained DCS facilities; to all government owned, contractor operated and maintained facilities and to all government leased DCS facilities for which the government provides physical security protection. This standard serves as a guideline for the physical security protection of other government leased DCS facilities. This standard provides the requirements and information for retrofitting existing DCS facilities and designing new facilities.

1.3 Implementation

1.3.1 Security Program

A physical security program will be implemented for each facility serving the DCS. Each command or agency having responsibility for the operation and maintenance of such a facility, and each procurement activity that procures the services of contractors to operate and maintain such a facility shall prepare and implement a physical security program for each site to meet the security program requirements contained herein.

1.3.2 Applicability

This standard provides requirements, procedures, and methods for implementing a physical security program at DCS facilities. While the program will vary to a certain degree, on a site-by-site basis, certain minimum standards must be achieved to provide a minimum degree of protection.

This standard provides physical security requirements analysis procedures which shall be undertaken for all DCS sites. This standard also provides a variety of physical security measures which will be applied on a site by site basis to satisfy specific site physical security requirements. Implementation of this military standard shall apply to newly constructed facilities and those undergoing major reconfiguration. It should be applicable as guidance for upgrading existing sites.

This standard addresses threats against DCS sites which can be manifested by vandals, terrorists, saboteurs, and special operations forces. These are the most immediate and inherent threats against DCS facilities.

1.3.3 Compatibility

Efforts have been made to assure that the provisions of this standard are compatible with other requirements affecting the design, operation and maintenance of DCS facilities. In particular, attention has been given to assuring that this standard is compatible with other DCS survivability requirements. Where unavoidable conflicts arise between this standard and other requirements, each operating command or agency will prioritize their requirements based on (1) mission importance, to include availability of backup systems, (2) the hostile threat both for peacetime and wartime (3) vulnerability, to include inherent local vulnerabilities

and geographic location, whether in a remote or populated area. The prioritization and related compensatory security measures will be accomplished on a site-by-site basis with the coordination and approval of the host Security/Military Police or equivalent agency.

1.3.4 Organization of Standard. This standard has been prepared to meet the requirements, as closely as possible, of MIL-STD-962, "Outline of Forms and Instructions for the Preparation of Military Standards and Military Handbooks." As a result the information is provided in a specific format.

2. REFERENCED DOCUMENTS

2.1 Issues of Documents. The following documents of the issue in effect on date of invitation for bids or request for proposal, form a part of this standard to the extent specified herein.

Specifications

Federal

RR-F-191/1, Type I	Chain-Link Fence

Military

MIL-B-52775A	Barbed Tape
MIL-P-43607E	Padlock, Key Operated, High Security, Shrouded Shackle
MIL-R-7705A	Radomes, General Specifications for

2.2 Other Publications. The following documents form a part of this standard to the extent specified herein. Unless otherwise indicated, the issue in effect on date of invitation for bids or request for proposal shall apply.

Army

USA Field Manual 19-30	Physical Security
USA Office, Chief of Engineers Drawing 40-16-10	Chain Link Fence
USA Material Command, AMCP 706-185, Engineering Handbook	Military Pyrotechnics Series, Part I Theory and Application

Navy

USN, OPNAV Instruction 5510.45B	Physical Security Manual

Air Force

AFR 207-1	The Air Force Physical Security Program
USAF HQ, AFCC/DEO	Construction Design Criteria for the Protection of Air Force Operated DCS Sites

Department of Energy

Intrusion Detection Systems Handbook, Volumes I and II	Information Systems Department 1700, Sandia Laboratories, Albuquerque, New Mexico
Barrier Technology Handbook	*Nuclear Security* Systems - 1700, Sandia Laboratories, Albuquerque, New Mexico

Other

National Cooperative Highway Reserach Program Report 54, Location, Selection and Maintenance of Highway Guardrails and Median Barriers	Southwest Research Institute, San Antonio, Texas

3. DEFINITIONS

3.1 Allocation. The setting apart, or designating resources for a specific purpose. In physical security planning, the allocation process results in designating security resources to protect against identified vulnerabilities.

3.2 Barriers. Fences, walls, or other obstructions specifically designed to deter and prevent penetration into DCS sites.

3.3 Chemical Weapons. Anti-personnel weapons that achieve casualties through chemical interactions with the human body.

3.4 Cold War. A conflict carried on by methods short of sustained overt military action.

3.5 Conventional Weapons. Weapons that achieve their destructive effect upon a target through the use of chemical explosives an /or warhead fragmentation. Not included in conventional weapons are those that use nuclear explosives, or chemical (CBR) weapons.

3.6 Criticality. The importance of a communication site or facility judged according to the need for the site or facility in providing essential communication during crises.

3.7 Damage. That degree of degradation of operational capability caused by physical destruction to a DCS sites' personnel, structures, and equipment.

3.8 Deceit. Actions taken by an adversary to defeat physical security measures with the expectation that unauthorized conditions, such as false credentials, will not be detected.

3.9 Delay. The additional amount of time required by an intruder to accomplish a specific task, as a result of the implementation of security measures.

3.10 Denial. The act or process of negating the ability of an intruder to enter or damage a site and its component equipment.

3.11 Detection. The act or process of determining the presence of an intruder. In electronic systems, the process of determining the presence of a signal.

3.12 Deterrence. The act or process of inhibiting intrusion into a communications site. Deterrence may be accomplished by either psychological or physical means.

3.13 Disruption is the lowest level of damage. Disruption may be caused immediately by damage to some vital part of the communications equipment. Disruption may be delayed by causing damage to local standby power and later interrupting commercial power. Damage included under disruption must be able to be repaired within 3 hours by normal service personnel with readily available tools and components.

3.14 Endurability. The capability of a DCS site to maintain essential connectivity for a specified period of time immediately following commencement of stress infliction upon the site.

3.15 Explosives. Chemical substances which release large amounts of energy in very short periods of time, resulting in the creation of high

local pressures. Included under the term explosives are special configurations of explosive substances to cut or destroy material through blast and shock effects.

3.16 Facility. The integrated collection of buildings, equipment, and personnel, located at a site, to accomplish a communications mission.

3.17 False Alarm (Electronic). The triggering of an electric or electronic alarm system due to random electronic events within the electronic system itself.

3.18 False Alarm Rate. The number of false alarms that occur per unit time. The false alarm rate is usually expressed as events per second, per hour, or per day, and includes electronic and nuisance sources.

3.19 Force. Actions taken by an adversary to defeat physical security measures by overt aggressive activities.

3.20 Foreign Agent(s). A person or group of persons in the employ of a foreign, hostile state who threaten(s) the operations, facilities, or personnel of the DCS with damage and/or destruction to disrupt DCS operations and/or embarrass the U.S. host country.

3.21 Functional Equipment. Electronic equipment or supporting equipment necessary for the facility to provide its communication function. This typically includes antennas, waveguides, cables, receivers, multiplexers, transmitters, power supplies, and cooling equipment.

3.22 General War. Warfare between nations in which the total resources of the nations may be utilized or targeted.

3.23 Generic Site. A communications site, containing all elements of signal reception, processing, and transmission, with provisions for emergency power, and contained in a single parcel of cleared flat land which is not occupied by other noncommunications tenants or operations.

3.24 Guard Force. A unit of personnel equipped, trained and organized to provide security for a site, facility or operation.

3.25 Hardening. The process of installing systems or implementing measures to render a communications site more difficult to enter or more difficult to damage and destroy.

3.26 Intrusion. The act of wrongfully entering into a communications site or facility.

3.27 Intrusion Detection Systems. Sensor systems emplaced to detect intrusion into a DCS site and relay that information to appropriate personnel.

3.28 Life Cycle. The total phases through which an item or system passes from the time it is intially developed until the time it is either consumed or disposed of as being excess to known requirements. Applied to DCS sites it is the sequence of events included in the planning, development, installation, operation, maintenance, and eventual retirement of a communications facility and equipment, including equipment to provide security.

3.29 Manned Site. A communications site at which personnel are present continuously.

3.30 Matrix. A rectangular array of information arranged in rows and columns to show the relationship or connections between the items of information. Depending upon the kinds of information contained in the

matrix, the elements may be subject to defined mathematical operations such as addition, subtraction, and multiplication.

3.31 Nuclear Weapons. Weapons which produce their energy release through nuclear fission or fusion reactions.

3.32 Nuisance False Alarm (Non-Electronic). The triggering of an electric or electronic alarm system due to the presence of a nonthreatening intrusion. An example is the triggering of a sensor due to animals or seismic activity. The cause of a nuisance alarm is always due to a cause outside of the sensor system itself.

3.33 Operating Activity. The agency, organization, or command which has overall operations and maintenance responsibility for a DCS facility or installation.

3.34 Peacetime. A period of time in which the United States is not engaged in armed conflict.

3.35 Physical Security. The condition of being protected from injury, harm or loss due to deliberate physical attack against personnel, equipment, or facilities.

Alternatively: That part of security (operations) concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft. (JCS Pub 1).

3.36 Physical Security Measures. Actions taken to protect from or lessen the effects of physical attacks upon personnel, equipment or facilities. Physical security measures may include the use of sensors, locks, barriers, procedures and guard forces.

3.37 Procedural Security. The management constraints; operational, administrative and accountability procedures; and supplemental controls established to provide an acceptable level of protection.

3.38 Protective Lighting. The provision of visible illumination, during hours of darkness, as an aid for intrusion detection and verification by optical systems or security personnel.

3.39 Readiness. The state of being immediately and perpetually prepared to respond to all acts or potential acts of harm against the facility.

3.40 Real Time Assessment. The verification of the cause of an alarm while the alarm is being activated.

3.41 Required Response Time. The time between when an intruder has set off a validated alarm and when he could penetrate enough barriers to cause disruption of services.

3.42 Response Force. Guards, security personnel, or operations personnel whose purpose is to intercept and/or delay an intruder possibly through the use of force, including lethal force.

3.43 Response Force Response Time. The time required for the response force to travel to the site, measured from the receipt of a validated alarm.

3.44 Sabotage. The deliberate, clandestine destruction, damage, or obstruction by any means, of installations, equipments, or facilities essential to the national security of the United States primarily by individuals acting in the interests of a foreign power or subversive political organization.

3.45 Saboteur. An individual, acting for the interests of a foreign power or subversive political organization, who willfully causes damage or destruction of equipment and facilities, and who intends to harm the national security of the United States. A saboteur is always considered trained and equipped for a specific mission.

3.46 Safety. The condition of being protected from injury, harm or loss due to accidental causes. Alternatively - a device or system designed to prevent inadvertent or hazardous operations.

3.47 Security. The condition of being protected from injury, harm or loss due to deliberate actions or attacks.

3.48 Security Program. That set of activities, including planning, budgeting, procurement, operations, maintenance, inspection, and evaluation, required to provide security.

3.49 Site. A parcel of land, and the buildings and equipment thereon, which comprise a communications facility.

3.50 Site Classification. The process of designating a site as generic or unique. The results of classifying a site according to its characteristics.

3.51 Site Security Force. Personnel who are specifically trained, organized and assigned to perform security duties at a specific site or facility.

3.52 Small Arms Fire. Gunfire from weapons whose caliber is 40MM or less, and which have essentially line-of-sight trajectories.

3.53 Special Operations Forces (SOFs). Hostile military forces operating in small teams trained to conduct unconventional warfare operations from peacetime through war against the DCS with the aim of damaging and/or disrupting the operations of critical DCS facilities.

3.54 Stealth. Actions taken by an intruder to prevent detection by intrusion sensor systems or by security force personnel.

3.55 Survivability. The ability to withstand the effects of an attack to the extent that essential functions can be resumed after the attack.

3.56 Temporary Functional Destruction. The physical condition characterized by minor damage to vital parts of the system that require short lead times to repair or replace. Typically all functional equipment damaged would not have to be replaced and emergency repair could be made on site.

3.57 Terrorist(s). A person or group of persons motivated by political interests which are derived from foreign or domestic ideologies or political developments or some combination thereof. Terrorist(s) may or may not be trained for a specific mission. The intention is to threaten, or actually assault personnel and/or damage equipment and facilities to influence political behavior by this type of action(s).

3.58 Threat. The threat to the DCS is defined as any action taken by an individual or group possessing the intent and capability to damage and/or destroy a manned or unmanned DCS facility or any portion thereof.

3.59 Tools. Implements, devices or chemicals used to facilitate entry or cause damage to a site or the equipment contained thereon.

3.60 Total Functional Destruction is characterized by damage to vital parts of the system that require long lead times to replace. Typically all functional equipment would be damaged and have to be replaced.

3.61 Unique Site. A communications site that does not qualify as a generic site. Examples of unique sites include an underground communications site, a building occupied jointly with other non-communications activities, or facilities occupying more than one distinct parcel of land.

3.62 Unmanned Site. A communications site at which no personnel are present continuously. Personnel attend to the operation of equipment only on a periodic maintenance, or an on-call repair basis.

3.63 Using Organization/Activity. The agency, organization or command which the operating command supports to fulfill the mission.

3.64 Validated Alarm. The accumulated indications which confirm the presence of an intruder in a DCS site.

3.65 Vandal(s). An individual who intrudes or causes damage as a prank, as retribution for a personal grievance, or for his own benefit, entertainment or satisfaction.

3.66 Vulnerability. The potentiality for damage or destruction based upon an integrated evaluation of a site's susceptibilities, and a threat's capability to exploit the susceptibilities.

3.67 Weapons. An implement or instrument, designed or adapted for the injury or killing of personnel, or to the damaging and destruction of equipments, facilities, or other physical resources.

3.68 Zones. Continuous regions delineated by boundaries which surround the components and equipments.

4. GENERAL REQUIREMENTS

4.1 Policy

4.1.1 Application. The requirements, for the physical security of DCS facilities, detailed herein are applicable to existing and newly constructed facilities. The requirements are mandatory for construction of new DCS facilities. The requirements of this standard will be considered for upgrade actions based on (1) mission criticality (2) hostile threat and (3) individual site vulnerability and will be included in the operation and maintenance of all DCS facilities.

4.1.2 Priorities. The allocation of resources to provide physical security at DCS facilities shall be done to assure the security of mission essential facilities. The allocation of resources (funds, personnel, and material) between facilities shall be done by the using commands to assure security of the mission essential facilities as a first priority. Allocation of resources to a given site shall be based upon the systematic analysis of (a) mission importance (Security Priority) (availability of backup systems, redundancy and alternate routing); (b) the hostile threat (terrorist or local dissident groups, availability of explosives, availability of firearms and crisis/wartime threat to the resources); and (c) vulnerability (remoteness, nearness to populated areas, and availability of security forces). This process is described in subsequent sections of this standard.

4.1.3 Security Program. Resources, to implement site security measures, shall be apportioned toward the implementation of such measures based upon a comprehensive assessment of the relative contribution a given security measure provides in meeting the overall security program objectives. The assessment shall address all relevant factors including the threat, site security/endurability objectives, available resources, feasibility of candidate security measures, their relative effectiveness, and implementation cost. Based upon the results of the assessment a comprehensive security program plan shall be prepared for each site. This plan is described further in Sections 4.3.1 and 5.3 of this standard.

4.1.4 Personnel. The using activities of DCS facilities shall be responsible for identification of the occupational skills required to establish, operate and maintain the physical security program detailed herein. In general, it is not expected that occupational skills beyond the standard military occupational skills in communications, civil engineering, security, and military police are required.

Upon establishment of the required physical security program, it is the responsibility of the operating command to conduct the required training for security program effectiveness.

4.1.5 Site Size. The physical size of a communications facility determines in large measure the feasibility and the cost of providing adequate physical security. In general, every effort shall be made to reduce the area or areas encompassed by DCS facilities to eliminate requirements to secure unnecessary terrain but still implement adequate security measures.

Where a DCS facility occupies a large area, efforts shall be made to subdivide and compartment essential facilities into zones providing requisite levels of protection. The process of dividing a site into security zones is described in Section 4.3.3.4 of this standard.

4.1.6 Inspection. The physical security program established in fulfillment of the requirements of this standard shall include review of the physical security program plan, and the implementation and inspection of physical security measures themselves. Security inspections shall be scheduled to provide formal inspections on a yearly basis, and more frequent informal inspections as the local mission and threat dictate. Security program reviews and security system inspections shall be accomplished within thirty days after the completion of any site modifications that affect the physical security equipment or procedures.

4.1.7 Intelligence. Operating activities shall establish and maintain close and frequent liaison with local intelligence units, with intelligence units supporting the operating command, military police and security forces having jurisdiction in the area of the site. Operating activities shall establish and maintain a record or log book describing and documenting attempts or actual incidents of vandalism, unauthorized entry to sites, sabotage, or surveillance conducted against a site. Intelligence, counter-intelligence, and supporting security units shall be informed of all such incidents.

4.1.8 Foreign National Sovereignty. DCS facilities located outside the United States may be located on property not under the sovereign control of the United States. The implementation of security measures at such sites may be limited by status-of-forces agreements between a host nation and the United States. Using/operating activities will review

terms of agreements to determine the contents and limitation of any security procedures/practices in effect in the host country. The reviews will be conducted by the host Security/Military Police unit, representatives of the communication facility, legal and planning offices and other representatives having expressed interest in the overall mission and site operation. Operating activities shall assure that all latitude available in status-of-forces agreements is utilized in preparing physical security program plans.

Operating activities shall assure that no physical security measure is implemented which conflicts with local status-of-forces agreements.

Operating activities shall coordinate with local area or theater commanders, and U.S. Consulate officers to determine the relevant terms of status-of-forces agreements.

4.2 Security Program Requirements

4.2.1 General. A security program is required for each site within the DCS. This required security program shall be tailored for each individual site. The site-by-site tailoring shall entail making certain determinations, evaluations, and assessments of various activities to be addressed in the security program. These activities shall include as a minimum: a threat assessment, determination of site susceptibilities, a vulnerability assessment, evaluation of site criticality and endurability requirements, determination of appropriate physical security measures and available options, development of an implementation plan, security procedures for on-going operations, and a plan for the allocation of protection measure resources to accomplish the security program objectives.

4.2.2 Threat Assessment. The threat posed against a given DCS facility depends upon the geographical location of this facility, the political and economic environment in the area, and the function the facility has in varying scenarios. The operating command and using activity shall obtain from the appropriate intelligence support agency or detachment, the nature and capabilities of the threat to a site. A profile of the threat shall be developed for each site. This threat profile shall identify, in as much detail as necessary, an identification of persons, groups or organizations, and foreign agents who constitute a probable threat to a site. The threat profile shall contain enough detail on threat organization, training, equipment, and motivation to permit an evaluation of the probable effectiveness of candidate security measures. The threat profile shall include consideration of the threat posed by vandals, political demonstrators, terrorists and saboteurs, and shall consider the scenarios of peacetime and periods of pre-hostility tension.

4.2.3 Site Susceptibilities. Each DCS facility requires the continuous functioning of specific operations such as power generation or conversion, signal transmission and reception, and data processing. Disruption or loss of a single such operation leads to loss of capability and mission failure of the site. Through use of site operational flow diagrams, fault tree analyses shall be performed to identify the failure modes of a given facility. The identified failure modes shall be compared with the actual physical layout and integration of the site to arrive at site susceptibilities. Site susceptibilities are the ways the facility may be damaged to cause loss of facility function.

4.2.4 Site Criticality and Endurability Requirements. Each individual facility within the DCS serves a different mission. This mission varies depending upon the location, the scenario, the subscribers served, the kind of communication media involved, and the degree of redundancy in the network. The operating activity, in coordination with the DCA, shall perform a mission analysis to arrive at a statement of site criticality and the site endurability requirements. The statement of criticality shall be used to prioritize the allocation of physical security resources. Both site criticality and endurability requirements shall be referred to when evaluating the effectiveness of the site physical security program.

4.2.5 Determination of Appropriate Security Measures. The security measures to be implemented at a given site are to be determined on a case-by-case basis. The factors to be considered are the threat, the site susceptibilities, mission importance (site criticality), and endurability requirements. The methodology for the systematic consideration of these factors is given in subsequent sections of this standard.

4.2.6 Allocation of Resources. Using commands shall prepare a plan for the allocation of available resources for providing physical security at each site. The resources allocation plan shall cover both the installation and operational phases of the site security program. The plan shall include consideration of the utilization of financial, material, and personnel resources. Portions of the plan requiring the provision of services or responses by security or military police shall be coordinated and approved by such police units.

4.3 User Implementation - General Instructions

4.3.1 Security Program Plan. Responsible operating activities shall prepare a security program tailored to the security needs of each DCS site. The detailed requirements for the security program plan are provided in section 5.3 of this standard. The security program plan will be developed through an in-depth analysis of assessments, evaluations and determinations of elements of information to be included in the security program plan. In general, the security program plan shall include the following elements of information: a threat analysis, site susceptibility analysis, vulnerability analysis, site criticality analysis, endurability criteria, physical security measure options, allocation of protection measure resources, security effectiveness analysis, implementation plan, and security procedures to maintain on-going operations.

4.3.2 Site Classification. The operating activities shall determine the classification of a site as being generic or unique. Using the definitions of generic or unique sites given in sections 3.22 and 3.58 above, along with other considerations that may be appropriate, a determination shall be made as to whether a given site may be classified as a unique or generic site. If a site can be classified as being generic, then the procedures and methods for physical security protection given in section 5.1 shall be applied. If a site is classified as being unique then the procedures in section 5.2 shall be applied.

4.3.3 Security Measures

4.3.3.1 Concept. The overall approach to providing security in DCS sites consists of five elements. These elements of the security system

are intrusion deterrence, intrusion detection, alarm assessment, component and physical plant hardening, and security or response force personnel. The intrusion deterrence element is intended to provide a psychological state of mind to a potential intruder that an intrusion will result in an unacceptable counteraction. The intrusion detection element is intended to provide an alarm to the operating activity or security personnel that an unauthorized intrusion has occured at a DCS site. The alarm assessment element is intended to verify that an intrusion alarm was activated by a threat against the DCS site. The component hardening element of the physical security system is intended to cause delay in the accomplishment of damages or to limit the amount of damage that may be inflicted upon a site. The security force element is intended to delay, stop or mitigate the actions of an intruder. Every DCS site security program shall be prepared to include the five elements of the security system.

4.3.3.2 Physical Security Measures. The physical security system for a DCS site may consist of a combination of passive and active measures, coupled to the utilization of response forces.

4.3.3.2.1 Passive Measures. Passive security measures consist of those measures which do not consume energy after their initial installation. Included in the category of passive measures are fences, barriers, revetments, walls and hardening measures that delay or deter intruders.

4.3.3.2.2 Active Measures. Active physical security measures consist of the use of sensors and devices, which require the consumption of energy after installation or involve human activity for effectiveness. Active measures may both deter or delay an intruder. Active measures

include intrusion sensors, protective lighting, smoke or other obscurants, or sprays and foams. It is essential that the use of foams be restricted for use outside the equipment areas.

4.3.3.2.3 Response Force. It is highly preferable that the response force consist of trained security forces. Due to manpower allocations, site remoteness, budget constraints, etc., this is not always possible. It may be necessary, in some instances, to utilize guards, operations personnel or security personnel to act in this capacity.

These individuals shall be organized to respond as a unit, and trained in the use of firearms and lethal force. Since these individuals will often serve on the response force as an additional duty, their training and testing will require special planning and scheduling. Response force personnel should be made thoroughly familiar with the facilities they will be called upon to protect. Training exercises should be conducted at the sites to be protected.

When response force personnel include site operating personnel, such personnel should be utilized in the planning of response force activities to make maximum use of their intimate knowledge of site layout and susceptibilities.

4.3.3.3 Procedural Security Measures. Procedural security measures consist of those human activities which have been planned or implemented to enhance, or complement physical security measures. Procedural security measures include site entry control, alarm assessment procedures, on-site weapon control, and guard force duties. Procedural security measures are generally those directives issued by a local commander to cause best utilization of security resources at a given site.

4.3.3.3.1 Enforcement of Security Measures and Procedures. Security measures and procedures can be rendered ineffective if they are not properly enforced. It shall be the responsibility of both the operating and using activity to establish enforcement procedures at the DCS site(s). These enforcement procedures shall be developed to meet the requirements of the MIL-STD and to satisfy the needs of the authority responsible for the security of the site. Enforcement methods need to be developed to address those "Procedural Measures" stated in paragraph 4.3.3.3 of this standard.

4.3.3.4 Concept of Security Zones. The protection of a DCS site shall consist of implementing security measures, both physical and procedural, within each of 5 separate areas that together encompass the entire site and its immediate surroundings. These areas and their boundaries constitute security zones as defined below.

4.3.3.4.1 Definition. Security zones are continuous regions, delineated by boundaries, that surround the components and equipments to be protected. Each site is comprised of 5 security zones (Zones 0, 1, 2, 3, and 4). Boundaries between security zones will in most cases consist of barriers that impede the progress of intruders. The actual sizes of security zones are a function of the individual site. Examples of security zones at generic DCS sites are presented in Figures 1 and 2 of this standard.

The several zones and the security measures incorporated therein are configured to achieve physical security protection along the following hierarchy of effects against potential threat:

4.3.3.4.2 Rationale. Security measures are implemented using the concept of security zones to produce a defense-in-depth for the protection of a DCS facility and to facilitate the assessment of security effectiveness by providing well defined zones for the application and evaluation of physical protection.

The several zones and the security measures incorporated therein are configured to achieve physical security protection along the following hierarchy of effects against a potential threat:

		Security Measure Goals
Zone 0	-	Improved Observation
Zone 1	-	Deterrence
Zone 2	-	Deterrence and Detection
Zone 3	-	Detection and Delay
Zone 4	-	Delay and Apprehension

4.3.3.4.3 Application. Security measures shall be applied to each of 5 security zones resulting in a defense-in-depth consisting of a number of distinct countermeasures that an intruder must defeat in sequence in order to reach the intended target. Defense-in-depth is achieved by siting concentric sensor systems and barriers so that they successfully detect an intrusion and sufficiently delay the intruder so that he can be interdicted by an appropriate response force. Specific guidelines for generic sites are provided in paragraphs 5.1.3.2 through 5.1.3.6.

4.3.3.4.4 Impact. Security measures applied to each security zone shall have one or all of the following impacts:

a. Improved observation.

b. Provide intrusion deterrence by producing an obstacle, real or imaginary, to a potential intruder.

c. Increase intrusion delay by increasing the time required by the intruder to penetrate barriers in order to reach his intended target and by burdening the intruder with special or increased equipment needed to penetrate the barrier.

d. Facilitate intrusion detection by providing effective locations for the placement of sensors.

e. Facilitate alarm assessment by providing well defined regions for visual or audio interrogation of sensed intrusions.

f. Enhance effectiveness of security forces by increasing the probability of intrusion detection and by providing sufficient intrusion delay to allow an effective and timely response to an intrusion.

4.3.3.4.5 Characteristics. The following characteristics apply to security zones:

a. Security zones shall be numbered with the highest zone number corresponding to the most secure region of the facility.

b. Each security zone shall consist of a continuous region surrounding the components and equipments to be protected.

c. Adjacent zones shall have zone numbers that differ by not more than one.

d. There may be more than one security zone with the same zone number provided that the preceding condition holds.

e. All sites shall have 5 security zones.

f. The number and location of security zones are independent of the threat.

g. Security barriers consist of security fences, reinforced concrete barriers, walls, domes, and special reinforced concrete or metal sleeves.

h. Security measures applied to security zone boundary openings (gates and doors) shall be commensurate with those applied to the zone boundary.

4.3.3.4.6 Zone 0. Zone 0 consists of the region outside the perimeter fence. Zone 0 typically contains the following site elements:

a. Cleared land outside the perimeter fence.

b. Access road.

c. Parking lots.

d. Commercial power lines.

e. Guy wires.

The primary benefits of security measures installed in Zone 0 are improvements in alarm assessment and deterrence and detection of vehicular intrusions. For example, the cleared area outside the perimeter fence facilitates visual assessment of intrusion while a sensored gate in an access road deters and detects vehicle penetration.

4.3.3.4.7 Zone 1. Zone 1 includes the perimeter fence and the region between the perimeter fence and an inner fence. Site elements contained in Zone 1 include the following:

a. Perimeter fence, gate, and locks.

b. Cleared area between perimeter and inner fence.

c. Warning signs.

d. Sensors.

The primary benefits of security measures installed in Zone 1 are deterrence and detection of intrusions and improved alarm assessment. For example, the perimeter fence deters casual intrusion, a sensor line in the Zone 1 cleared area detects fence penetration, and the cleared area facilitates visual assessment of intrusion.

4.3.3.4.8 Zone 2. Zone 2 includes the inner fence, and the area between the inner fence and the outer barriers needed to protect towers, antennas, power sources, and electronic equipment. Zone 2 site elements include:

a. Inner fence, gates, and locks.

b. Sensors on the inner fence.

c. Perimeter lighting.

d. Closed circuit television.

e. Communication cables.

f. Fuel storage.

g. Fuel lines.

The primary benefits of security measures installed in Zone 2 are intrusion detection and improved alarm assessment. For example, the sensors on the Zone 2 inner fence detect intrusion while the Zone 2 perimeter lighting and closed circuit television facilitate alarm assessment.

4.3.3.4.9 Zone 3. Zone 3 includes the outer barriers and the area between the outer barriers and the inner barriers needed to protect towers, antennas, power sources, and electronic equipment. Site elements contained in Zone 3 include the following:

a. Outer barriers, for example, concrete block walls.

b. Area between the outer barriers and the inner barriers.

c. Waveguides

d. Antennas and antenna feeds

e. Heating, ventilation and air conditioning.

The primary benefit of security measures installed in Zone 3 is intrusion delay to facilitate interception by a response force. For example, a reinforced concrete barrier will require added penetration time and require that the intruder carry special penetration equipment such as tools or explosives.

4.3.3.4.10 Zone 4. Zone 4 includes the inner barriers needed to protect towers, antennas, power and fuel sources, and electronic equipment and the area within the inner barriers. Site elements contained in Zone 4 include the following:

a. Inner barrier.

b. Area within the inner barriers.

c. Towers and tower legs

d. Guy wires and guy wire anchors.

e. Electronic equipment.

f. Power and fuel sources.

The primary benefit of security measures in Zone 4 is intrusion delay which allows more time for interception by a response force before critical assets are damaged. For example, special concrete sleeves around tower legs will require added penetration time and require that the intruder carry special penetration equipment. Placement of equipment in vaults will require a major effort by an intruder to damage the equipment.

4.3.3.4.11 Variability. Physical barriers should be used to delineate security zones. However, some facilities may not have a sufficient number of physical barriers to delineate 5 zones as defined above. For

example, there may be only one perimeter fence at a site due to inadequate site area. For sites where a sufficient number of barriers cannot be implemented, the zones shall be delineated by the feasible barriers and security measures will be implemented within the zones to achieve a defense-in-depth. The zones shall also be chosen to match the descriptions in 4.3.3.4.6 through 4.3.3.4.10 as closely as possible. Additional physical and procedural security measures shall be implemented on or near the existing barriers commensurate with the levels of deterrence, detection, or delay that would have been provided if additional barriers were in place. This procedure ensures that all DCS facilities will have a layered physical security system regardless of the number of physical barriers available. It also ensures that the level of protection afforded a site with an insufficient number of barriers is commensurate with that for a site with physical barriers delineating all 5 zones.

4.3.4 Security Measure Effectiveness. Each security program plan shall contain within it the criteria for evaluating the effectiveness of the security measures to be implemented. In general the effectiveness of security measures implemented at DCS facilities shall be measured according to the degree of deterrence, the amount of delay, or the degree of damage limitation provided by the security measures. The effectiveness of security measures shall be assessed for their individual performance or contribution to site security, as well as their performance in conjunction with other security measures. For example, the effectiveness or value of sensors should be evaluated both with and without the use of barriers and vaults, or with and without the availability of response forces.

4.3.4.1 Measures of Effectiveness

4.3.4.1.1 Deterrence Effectiveness. The deterrence effectiveness of a given security measure or combination of measures is not a quantifiable parameter. To ascertain the deterrence effectiveness of a given measure against a specified threat, security planners should refer to the experience gained at other nearby facilities utilizing similar security measures. Where no experience base is available, security planners should assume that security measures provide no deterrence to a dedicated terrorist or saboteur threat.

4.3.4.1.2 Delay Effectiveness. In general, most security measures provide some delay in the execution of damaging acts against a DCS facility. Delay effectiveness of a given security measure is quantified in terms of the additional time an intrusion or act of sabotage requires due to the presence or implementation of a given security measure. Security planners should assess the effectiveness of security measures taken singly and in combinations to arrive at the maximum possible effectiveness expected for a given set of security measures.

4.3.4.2.3 Damage Limitation Effectiveness. Some security measures have the effect of limiting the amount of damage that could be inflicted by a given threat. Damage limitation can be measured 1) in terms of the additional tasks (including explosives) required to achieve a given level of damage or 2) in terms of the site components and equipments that will have reduced damage as a result of implementing given security measures.

4.3.4.2 Response Force Time. Response force time is the time taken by an adequate security force to respond to an intrusion, measured from the first assessment of an intrusion alarm. In assessing security measure effectiveness (including the stationing of security forces), the

response force time must be less than the delay times provided by other security measures but in no case exceed 15 minutes. Because of geographic locations this is not always possible. Adequate compensatory measures will be developed or at a minimum the responsible using activity must provide a waiver to this requirement, renewable at one year intervals for a period not to exceed three years.

5. DETAILED REQUIREMENTS

5.1 Security Program Development - Generic Sites.

5.1.1 Threat Analysis. Worldwide Defense Communications Sites are potentially vulnerable to a number of distinct and serious physical security threats . A physical security threat to the DCS may be considered to be any action taken by an individual or group possessing the intent and capability to damage and/or destroy a manned or unmanned DCS facility or any portion thereof. The physical security threat is considered to be actions taken by persons in proximity to a DCS site or who enter thereon. Specifically excluded from the physical security threat are non-nuclear or nuclear operations involving conventional ground or air combat units. Specific threats to the DCS, considered in this military standard are those posed by vandals, terrorists, foreign agents, and special operations forces. These threat elements are defined in Section 3 Definitions.

5.1.1.1 Threat Categories. Threats to the DCS may be categorized according to the criteria presented below.

5.1.1.1.1 Threat Capabilities and Motives. Each of the threat forces considered to be of potential concern to DCS security -- vandals, terrorists, foreign agents, and SOFs -- possess unique capabilities to disrupt and/or destroy DCS facility operations and have specific motives for undertaking such actions. The motives and capabilities for each of these threat forces are presented below with appropriate commentary on

threat force size, mobility (range), level of expertise (training and tactics), and type of equipment and armament which potentially could be used by each type of threat force against the DCS. Table 1 summarizes the information presented below. DCS personnel involved in assessing the threat vulnerability of their specific DCS site(s) may require additional, classified documentation on threats (particularly on foreign agents and SOPs) in order to "size" the threat accurately for their specific type of site(s) and location(s).

Vandals: The threat of vandalism (and its associated subcategories of pilferage, theft, break-ins, and pranks) is the most common low-level peacetime threat faced by DCS facilities. Vandalism is unlike the other threat categories in which small groups of highly motivated, well-skilled individuals may deliberately attack a specific DCS target. Vandals generally operate alone and are not well-armed or skilled in techniques such as sabotage, demolition, etc. Nevertheless, they may be excellent marksmen by virtue of hunting experience and/or past military or guard service. Based on past incidents, therefore, the vandal threat may consist of: a disruptive intruder/trespasser; small objects thrown at the DCS facility (such as bricks, stones, etc.); fencecutting; removal of easily transportable, visible, on-site equipment; or shooting at the tower and/or parabolic dish. Such actions may be motiviated by a desire for personal material gain, excitement, or entertainment. Mental instability or political motives may also be contributing factors.

Terrorists: Terrorists may operate alone or in small teams of between 2 - 10 individuals who are assumed to be well-trained in sabotage-related skills, including the use of small arms and demolitions. The terrorist "arsenal" may include a variety of small arms and equipment,

including machine pistols, assault rifles, submachine guns, explosives detonating devices, hand grenades, smoke bombs, hand held rocket launchers, or mortars. A terrorist attack against a DCS facility would likely be motivated by a desire to publicize a specific cause (e.g. "anti-nuclear" sentiments, "anti-imperialism," etc.) and to achieve a psychological "victory" against the U.S. and/or the host country.

Foreign Agents: Foreign agents may act against the DCS either singly or, perhaps, in small teams. Agents are assumed to be well-trained experts who are skilled in the use of small arms (such as those listed for the terrorist "arsenal"). Soviet/Warsaw Pact agent activities against the DCS would likely have as their aim the disruption, damage, and/or destruction of DCS facilities as well as harrassment of the U.S. and/or the host country. Soviet/Warsaw Pact agents of probable concern to the security of DCS facilities include:

- Agent-diversant: tasked with sabotage missions;
- Agent-boyevik: tasked with shock-type actions or executive actions such as kidnapping;
- Agent spetsial'nogo naznacheniya: an agent usually tasked with a single, high priority assignment against one target (e.g., a critical DCS facility).

Special Operations Forces (SOFs): The Special Operations Forces (SOFs) threat encompasses the activities of diversionary brigades (groups, teams) and other unconventional warfare-related forces. The SOF threat to DCS facilities is a potentially serious one. This threat would begin at the time of transition from peacetime to war and would continue throughout the early phases of hostilities. SOFs would likely operate in

teams consisting of between 7-17 individuals. Team members would presumably be highly skilled in sabotage and related commando techniques. Their armament and equipment may include such items as anti-tank guns, snipers' rifles, assault rifles, grenade launchers, and rocket launchers. The primary objective of an SOF attack against a critical DCS facility would be its operational disruption and/or destruction to thwart U.S./NATO communications traffic and/or nuclear release commands throughout the period of hostilities.

5.1.1.1.2 Site Criticality and Location. Site criticality and location are factors which are directly interrelated with the type(s) of threat(s) posed to individual DCS facilities. The threat of vandalism, for example, is usually related to sites which are very isolated, in the vicinity of hunting grounds, and within close proximity to lands utilized by the public. Vandals would tend to select unmanned or lightly manned sites in remote areas because of their motivations.

Terrorists, on the other hand, might tend to select sites with very different characteristics regarding site criticality and location. Terrorist site targets, based on prior targets selected by terrorists for attack, would tend to be highly visible facilities which are obviously military (and, particularly, American) installations. Furthermore, analysis of terrorist incident data suggests that Western Europe, Latin America, and the Mid-East may be prime target areas based on past experience. These regions are thus the most likely locations where a terrorist assault may be expected against the DCS.

Foreign agents and Special Operations Forces (SOFs) would tend to select extremely critical sites in key locations as targets because of what is known about their missions. These critical nodes might be manned

or unmanned, and would be threatened particularly at the time of transition from peace to war. This would be particularly true for sites in Western Europe (and, in the Pacific Region, in South Korea) given existing scenarios for employment of threat forces.

In general, the criticality of a target site to the maintenance of communications connectivity would probably be well understood by terrorist or military threat forces (e.g. foreign agents and SOFs). Site location is an important factor regardless of the type of threat which is postulated. However, DCS personnel involved in identifying specific threats for their particular geographic location may require additional intelligence data from which threat probabilities may be derived.

5.1.1.2 Likelihood of Sabotage Attempt. In the allocation of resources for physical protection of DCS sites it would be helpful to know what the likelihood of a sabotage attempt might be. While DCS sites have been the target of vandalism and sabotage, there is no data to suggest the frequency with which sabotage has or will occur.

For physical security planning purposes, the planner shall assume that these DCS sites, possessing the greater criticality with respect to a network operation, will have a greater relative probability of being attacked. The relative probability of sabotage attack also depends upon the capabilities and location of threat elements. Therefore, in assessing the likelihood of sabotage attack, the security planner should obtain threat profile information from the appropriate intelligence support agency.

Where the sabotage threat eminates from a foreign power, the security planner shall assume the foreign power knows the role that a given site has within a DCS network.

In planning for physical security against a variety of threats, the planner should consider how the threat type changes with operational conditions. The security planner should expect that the relative probability of threat action is greatest by vandals and terroists during peacetime, and is least during periods of high international tension and actual war. Contrariwise, the planner should expect that the probability of threat action due to agents or special operations forces is least during peacetime and greatest during pre-conflict and wartime situations.

5.1.2 Generic Site Vulnerabilities. All of the communications sites and associated facilities identified with the Defense Communications System, whether government-owned or leased, can be categorized as being either generic or unique. Many of the sites are similar in size, shape, and topography of the terrain occupied. Further, the communications facilities and equipments are often identical. As a result of efforts in the standardization of site layouts and equipments, DCS sites tend to be similar and compact. For purposes of planning and implementing physical security programs, DCS sites are defined as being either generic or unique. A generic communications site is a site containing all of the essential elements of signal transmission, processing, and reception, and power generation (less commercial power) and contained in a single parcel of cleared, flat land, and which is not occupied by other noncommunications tenants or operations. All other sites are categorized as unique sites.

Physical security plannning and analysis for generic sites shall include the preparation and evaluation of a threat vulnerability matrix.

5.1.2.1 Threat Vulnerability Matrix. The threat vulnerability matrix for a site is an analytic tool for correlating the susceptibilities with a delineated threat to identify specific vulnerabilities which require physical security measures. The threat is delineated using procedures described in section 5.1.1 of this standard.

Each DCS site physical security program planner and implementer shall prepare a site specific threat vulnerability matrix, a comprehensive sample of which is given in Table 2. The left hand column lists all of the possible threat categories for DCS sites. The threats can range from casual intruder to a dedicated special forces team. Individual elements of the threat may be further defined in terms of the numbers of attackers, their equipment, and training. This latter information should be obtained from supporting intelligence and/or security units.

The upper row lists site susceptibilities that could be found at a typical DCS facility. This list is based upon surveys of numerous DCS sites. By definition, a site susceptibility is any element of the site that is essential to site operation and whose damage or destruction would eventually lead to cessation of site operations.

As shown in the matrix, susceptibilities may be delineated by security zones. This matrix has blank columns to allow the security planner to add additional susceptibilities based upon the survey of each specific site.

5.1.2.2 Use of Threat Vulnerability Matrix. In preparing the threat vulnerability matrix for each specific site, the security planner shall complete the following steps:

a. Identify and delineate the threats

b. Identify specific site susceptibilities

c. Correlate the threat with site susceptibilities.

The user of the matrix shall determine the nature and capabilities of the threat which may be posed against the specific site. This threat determination shall be obtained through coordination with the intelligence agency which supports the communications command. It shall include, not only projections of enemy capabilities, but also the results of operating experience at the site or similar facilities in the area. The total threat to each individual DCS site shall be described to a level of detail so that an identification of susceptibilities will be complete and reasonable.

The user of the threat vulnerability matrix shall divide the site into proposed or existing security zones as prescribed in Section 4.3.3.4. On the basis of an on-site survey and a site operations analysis the security planner shall identify and delineate by zones, the site susceptibilities. For cases in which the site is not yet constructed, the security planner may utilize site plans instead of an on-site survey. Even in this latter case, a visit to the intended site location is desirable to better define terrain and vegetation conditions.

Once the threat has been identified and delineated, and specific site susceptibilities defined and located by zones, the security planner shall prepare a threat vulnerability matrix as given in Table 2. Within the columns and rows of the matrix, the planner shall mark each box to indicate which susceptibility may be exploited by the identified threat element. When marking the threat vulnerability matrix, the qualitative probability of the threat-susceptibility interaction can be indicated by

marking the columns in the following manner: L - low probability, M - medium probability, and H - high probability, as shown in Table 2. These assessments will require coordination with the local intelligence unit. This qualitative assessment provides a basis for allocating physical security resources. When this process is completed the threat vulnerability matrix will identify specific site vulnerabilities where physical security protection should be allocated.

It may happen that the first draft of the threat vulnerability matrix will result in site susceptibilities requiring more protection than a particular zone provides. Under these circumstances, the zonal boundaries may be revised or additional security measures within a zone may be implemented to achieve greater protection for specific susceptibilities.

If the sample matrix is not sufficient to delineate all the threat elements and site susceptibilities, the site security planner should make additions to the matrix to describe the specific site situation.

5.1.2.3 Sample Threat Vulnerability Matrices. The following examples represent the results of applying the threat vulnerability procedures outlined above.

a. Unmanned Line-of-Sight Repeater in Alaska.

Table 3 presents a possible threat for an isolated microwave repeater (with self-supporting tower) in the White Alice Chain in Alaska. For this example it is assumed that the vandal threat consists solely of a single or group of hunters who are armed but do not carry any penetration tools. In this example there is no perceived terrorist or foreign agent threats for this site. However, the site serves as an important communications link in the region and, hence, would be an opportune target for a special operations force.

The threat-vulnerability matrix for this site is presented in Table 4. In preparing this matrix it was assumed that the susceptibilities were identified through a specific site survey. This must be considered when completing the matrix. For this case, power lines and waveguides are readily accessible except inside the communications building. Antennas and fuel tanks are exposed and hence highly vulnerable to weapons fire. The communications building is locked and of sufficient construction to prevent penetration by the unaided attacker. However, the building affords little protection to a dedicated team of saboteurs. Once inside, the saboteur has free access to the site's communications equipment and power sources.

b. Manned Satellite Ground Terminal in the Pacific.

Table 5 presents a possible threat for a manned satellite station in the Pacific region. This site is linked to other communications facilities by microwave LOS and by buried cable.

The site has a small on-site guard force which would preclude the vandal threat. A well-equipped terrorist group is active in the region and the possibility of an attempted site takeover is very real. It is assumed that the location of the site relative to garrisoned U.S. forces would prevent a special operations force from attacking the site. However, an attack by well armed in-place agents seems possible.

The threat-vulnerability matrix for this site is presented in Table 6. As in the prior example, it is assumed that susceptibilities were identified through a site survey. For this site, power lines and communication cables are readily accessible through unlocked cable vaults. Fuel tanks, fuel lines, waveguides, antennas

and antenna feeds are exposed and hence vulnerable to small arms fire. Although the site is guarded, the site is susceptible to a surprise attack by a small group of dedicated attackers who in turn could gain access to the communications and power buildings.

5.1.3 Security Measures Implementation - Detailed Instructions. In this section security measures to eliminate identified vulnerabilities on new or existing sites, are detailed along with instructions for their implementation.

5.1.3.1 Site Selection. The primary factors influencing the selection and modification of new and existing DCS site shall be the communications function of the particular DCS facility and the inherent defensibility of the chosen site.

5.1.3.1.1 Communications Function. The choice of site is related to the operational requirements of the communications link served by the site. Certain DCS functions may require towers to be placed on mountain tops or high promontories. Other DCS communication functions are less dependent on elevation. Once the topographical requirements have been established based on communications technology considerations, the final site selection shall be based on the defensibility of the location.

5.1.3.1.2 Site Modification. Both newly selected and existing sites shall be capable of being graded flat and cleared of all obstructions and vegetation to afford defending site personnel full fields of view and fire.

5.1.3.1.2.1 Site Location. Sites shall be located such that the entire site is level with or higher than surrounding territory for site defensive considerations. The grade of the summit upon which the site is located shall not be sufficiently severe to offer an intruder any reverse

cover or obstruct in any way a defender's full field of vision and fire. All the above mentioned considerations shall apply also to the site access road.

The DCS site shall not be surrounded or abutted by any natural or man made features higher in elevation than the ground level of the site itself because of the advantages which would accrue to hostiles' seizure of these features for the purposes of attacking the DCS site.

5.1.3.1.2.2 Water. A DCS site perimeter shall not border on any body of water sufficiently deep or wide to conceal a human swimmer.

5.1.3.1.2.3 Isolated Sites. Excessive isolation shall be justified only by the communications requirements of the particular sites concerned.

5.1.3.1.2.4 Response Forces. The availability and location of response forces shall be considered in the selection of a DCS site. The nature of the terrain separating the reaction forces from the site and the mobilization and transportation time required by the reaction force to reach an alerted site shall be major factors considered in the selection of a site.

5.1.3.1.2.5 DCS Sites Emplaced Upon Military Bases. If at all possible, DCS sites shall be located within the perimeters of a well situated, well defended U.S. or allied military base.

5.1.3.1.2.6 Urban Location. A DCS site located within an urban area shall not be located such that the site is surrounded by tall buildings. This shall not apply to existing sites which are so situated.

5.1.3.1.2.7 Local Threat Considerations. In a DCS site selection, the local threat shall be considered. If local conditions indicate a

high level of anti-American, anti-NATO, anti-friendly government, anti-military, or pro-Communist feeling among sections of the local indigenous or regularly transient population, every effort shall be made to avoid the location for a DCS site.

5.1.3.1.2.8 Geologic and Weather Conditions. Adverse geologic and weather conditions shall be reason for rejecting a potential site. The nature of the terrain, surface and subsurface, as well as local seismic conditions shall be considered thoroughly to assess the degree to which site components and functions, and site security equipment, may be partially or totally degraded.

5.1.3.2 Zone 0 Security Measures. Security measures in Zone 0 are implemented to deter and detect vehicular intrusions and to enhance visual observation.

5.1.3.2.1 Access Road Security Measures. The number of access roads at DCS facilities shall be kept to the minimum needed for efficient operation of the site.

5.1.3.2.1.1 Access Road. All access roads shall be lined continuously from the nearest adjacent road to the site perimeter fence gate by the vehicle barriers specified in Figure 3. Vehicle barriers shall not be used along a side of an access road if the terrain immediately adjacent to the road precludes the use of four wheel drive vehicles to circumvent the road. Vehicle barriers shall not be used to line the access road at facilities where the site perimeter is less than 60 m from an adjacent road or where the surrounding terrain offers alternative approaches to the site for four wheel drive vehicles. Vehicle barriers

shall be placed as shown in Figure 3 to prevent straight line approaches by vehicles to the perimeter fence or perimeter fence gate. Vehicle barriers shall be emplaced such that authorized access to a site by emergency or maintenance vehicles is still available.

5.1.3.2.1.2 Parking. Vehicle parking at manned DCS facilities shall be located more than 10 m outside the site perimeter fence. Vehicle barriers as specified in Figure 3 shall be placed around parking lots to prevent vehicular access to the perimeter fence. No vehicles shall be permitted within the site perimeter fence except those authorized for supply and maintenance purposes. No civilian vehicles shall be permitted within the site perimeter fence.

5.1.3.2.1.3 Entrance. Entrance to site access roads shall be restricted by the use of the vehicular control gate specified in Figure 4. The vehicular control gate shall be offset a minimum of 10 m from the adjacent road. A vehicular control gate shall not be used at facilities where the site perimeter is less than 60 m from an adjacent road or where the surrounding terrain offers alternative approaches to the site for four wheel drive vehicles. The vehicular control gate at unmanned sites shall remain locked at all times with the following exceptions:

a. If a maintenance crew is on site the vehicle control gate shall be closed but not locked to allow free passage of emergency vehicles should the need arise. When possible it is preferable to keep the gate locked, and to augment the maintenance crew with a person who could serve in a security and safety observation role during maintenance operations.

b. If the first response force to a site intrusion does not have the capability to unlock the vehicle control gate, the vehicular control gate may be closed but not locked. When possible it is preferable to lock the gate with a combination type security lock, with the combination being provided to the first response force by radio if gate opening is required.

At manned facilities, the vehicular control gate shall be closed except during periods of heavy traffic (for example, shift changes) and during normal visit and delivery times. The vehicular control gate at manned facilities shall not be locked in order to allow free passage of emergency vehicles. The vehicular control gate at both manned and unmanned DCS sites shall be posted with a warning sign as specified in paragraph 5.1.3.3.3.

5.1.3.2.1.4 Entrance Control. Access control for the vehicular control gate shall be accomplished using the site entry control procedures specified in paragraph 5.1.3.3.2 of this document.

5.1.3.2.2 Sensors. The access road sensor specified in Figure 5 shall be employed at all DCS facilities to sense vehicles approaching the site. An access road sensor shall not be used without a vehicular control gate that will preclude sightseeing or casual traffic from tripping the sensor. At unmanned facilities, the sensor output shall trigger an audible alarm on site as well as at the facilities charged with alarm assessments and response force dispatch for the site. At unmanned sites, the sensor shall not be deactivated at any time. At manned facilities, the sensor output shall trigger an audible alarm on site only. The alarm shall not be deactivated unless the vehicular control gate is opened to accommodate heavy traffic (see paragraph 5.1.3.2.1.3).

5.1.3.2.3 Alarm Assessment and Procedures. An alarm triggered by the access road sensor indicates the presence of a vehicle on the access road and inside the closed vehicular control gate. This vehicle presence will be either authorized and hence predicted according to the site entry procedure specified in paragaraph 5.1.3.3.2 or is unauthorized. At unmanned facilities, a response force shall be dispatched upon access road sensor alarm for an unauthorized vehicle's presence. If a maintenance crew is on site, visual assessment may be used to cancel said response action if warranted. At manned facilities, prompt visual assessment of an unauthorized vehicle shall be made, if possible, upon access road sensor alarm. If prompt visual assessment is not possible, for example at a site with a long access road, the nearest response force shall be dispatched upon access road sensor alarm.

5.1.3.2.4 Cleared Area. An extended cleared area of at least 9 m in width shall be maintained, outside the perimeter fence, through the use of chemicals or routine ground maintenance. The cleared area shall not have any obstacles, topographical features or vegetation greater than 20 cm in height. Where possible, topographical features and obstacles shall be removed to permit visual or enhanced visual (binoculars) assessment of access road sensor alarms.

5.1.3.2.5 Cables. All power, communications, and sensor cables entering the site and on-site shall be buried at least 1 meter. The locations of all buried cables shall be obscured. Where practical, cables shall enter the site via diverse routes. All manholes and cable vaults

on site shall be locked. Off-site, all power cables shall be buried to a distance from the site of at least 600 m. As a minimum, all manholes within that 600 m range shall be locked utilizing DoD approved high security padlock and key sets (see paragraph 5.1.3.3.5).

5.1.3.3 Zone 1 Security Measures. Security measures are installed in Zone 1 to provide intrusion deterrence and intrusion detection, and to enhance alarm assessment.

5.1.3.3.1 Perimeter Fence. All DCS sites shall be surrounded by a continuous perimeter fence as specified in Figure 6. New fences shall extend no less than 2.1 meters from the ground to the top of the fence fabric. Existing fences that are at least 1.8 m to the top of the fabric may be modified to the specifications shown in Figure 6, otherwise existing fences shall be replaced. The perimeter fence shall serve as a legal and physical demarcation of the restricted area boundary. The perimeter fence shall be located no less than 9 m from any facility or equipment critical to the operation of the DCS. The perimeter fence shall be located no less than 3 m from trees, poles, buildings, or other potential climbing aids that are inside the perimeter fence. The distance between the fence and outside trees, poles, buildings, or other potential climbing aids shall be greater than 9 m.

Fence fabric will be secured to fence posts with material equal to the tensil strength of the fencing itself. Metal mounting posts will be set in concrete and additional bracing as necessary will be provided at corners and gate openings. (Reinforced concrete posts may be substituted

if metal posts are not available.) All post bracings, etc., must be located on the inside (site side) of the fence fabric. The fences will be topped with a "Y" outrigger in accordance with figure 6B, with barbed wire and barbed tape.

Ground surface in the vicinity of the fence must be established in areas where loose sand or shifting soil exists or where surface water may cause erosion. Fences will not be erected on terrain with sharp contours, crossed with ditches, ravines, etc. A clear zone shall be established, in accordance with section 5.1.3.2.4, in all areas of both sides of the perimeter fence. No natural or man-made objects, capable of providing cover or concealment, shall be left standing in clear areas.

5.1.3.3.1.1 Drainage. Drainage shall be provided to prevent standing water from accumulating near the perimeter fence. All drain lines or culverts extending through the fence lines with cross-sectional area greater than 624 cm^2 and a smallest dimension greater than 16 cm shall be protected by a securely fastened or welded steel grid or replaced by multiple pipes of 25 cm diameter or 619 cm^2 area or less.

5.1.3.3.1.2 Signs. Warning signs as specified in paragraph 5.1.3.3.3 shall be posted at 30 m intervals along the perimeter fence. Warning signs shall be posted also on all gates. Signs shall be posted so that they do not obscure sizable portions of the perimeter fence and approaches thereto.

5.1.3.3.1.3 Gates. Vehicle and personnel gates shall be constructed as specified in Figure 7. The number of gates shall be kept to the minimum needed for efficient site operation. Only one entry point shall be established and its location shall be based on logical routes of travel into the site. Entry gates shall be positioned parallel to service or

main entry roads. Where entry through a gate is adjacent to heavily traveled roads, the gate shall be offset a minimum of 6 m from the edge of the road for vehicle safety. Gates not under security force observation shall be securable to the strength of the adjacent fence construction. Such gates shall be locked.

5.1.3.3.1.4 Entrance. At unmanned sites, vehicle and personnel gates shall be secured with high security padlocks (see paragraph 5.1.3.3.5). The procedures for entrance control are specified in paragraph 5.1.3.2.1.3.

5.1.3.3.1.5 Entrance Control. Access control for the vehicle and personnel gates shall be accomplished using the site entry control procedures specified in paragraph 5.1.3.3.2.

5.1.3.3.1.6 Entry Point Lighting. Entry point lighting shall be used at manned facilities for which entry controls are required during normal operations. Entry point lighting shall facilitate accurate and rapid identification of personnel requiring entry into the site. Two or more light fixtures shall be placed such that the light sources are above and behind the entry controller and face the person approaching the site. The intensity of the entry point lighting shall be not less than 16 lux for a distance no less than 15 m outward from the entry point.

5.1.3.3.2 Site Entry Control. Site entry control procedures shall be established to facilitate control of entry and exit of personnel and vehicles for both manned and unmanned DCS facilities according to the guidelines presented in paragraphs 5.1.3.3.2.1 and 5.1.3.3.2.2. Only authorized and essential personnel shall be allowed access to DCS sites. Authorization requirements shall be established according to the needs of

the individual DCS site (for example, security clearances). At no time shall an unauthorized individual be allowed access to any DCS site without continual escort by personnel empowered by the site commander to authorize the entry of said individual.

5.1.3.3.2.1 Unmanned Site. Entry control at an unmanned DCS site shall be accomplished by adopting a set of procedural guidelines with an overall objective of verifying the authority of each person seeking entry to a site. These guidelines shall consist of step-by-step instructions to be carried out by personnel requiring access to the site. As a minimum, these guidelines shall include the following steps:

a. Log books shall be established and maintained to record pertinent information regarding each site entry (for example, names of individuals, vehicle used, estimated and actual time in, time out, purpose of visit). Log books shall be kept at the facility charged with operation and maintenance responsibility of the unmanned DCS site and at the facility charged with dispatching a response force on sensor alarm. Log book entries shall be completed prior to and following each visit.

b. An estimated time of arrival on site shall be established for each visit and shall be adhered to as closely as possible. Alarms triggered by an authorized entry shall correlate with estimated time of arrival for logged site visits.

c. After entering onto a site, all gates shall be closed and locked according to the requirements specified in paragraphs 5.1.3.2.1.3 and 5.1.3.3.1.3.

d. As soon as possible after accessing the site, telephone contact shall be made with the facility charged with dispatching a response force on sensor alarms and with the facility charged with operating and maintenance responsibility. A prearranged code word or signal shall be passed to assure personnel are not being held hostage.

e. Upon exit, telephone contact shall be made with the facility charged with dispatching a response force and with the facility charged with operation and maintenance responsibility. All gates shall be locked after passage.

5.1.3.3.2.2 Manned Sites. Entry control at a manned DCS site shall be accomplished by adopting a set of procedural guidelines with the overall objective of verifying the authority of each person seeking entry to the site. These guidelines shall consist of step-by-step instructions for personnel and vehicle movement control. As a minimum, these guidelines shall include the following steps:

a. Access lists shall be established to identify personnel who have authorized and valid access rights commensurate with the security clearance requirements of the site. Access to a DCS site shall be limited to only those on the access list. Personnel not listed, who have a valid need for site access, shall be escorted at all times. A procedure shall be established to accommodate the immediate removal, from all access rosters, the names of terminated employees, contractors, and other personnel no longer authorized access to the facility. On-site guards shall not be used for escort.

b. A procedure shall be established for positive identification of persons authorized access to the site. This procedure shall consist of the use of security identification cards and badges. However, for small sites, personal recognition may be used if that person's name is currently on the access roster.

c. If an on-site guard is posted at a entry gate, said guard shall make visual assessments of all personnel requesting entry to the site. The guard shall have available to him a fixed or portable duress alarm. The duress alarm will terminate at a Security/ Military Police (or other Security) Control Center when available. When this is not possible, the duress alarm will terminate within the site at a manned location capable of assessing, responding or transmitting the call for duress to a security force capable of responding to the site.

d. For sites where an on-site guard is not posted at an entry gate for 24 hours a day, a call box or intercom shall be maintained at the perimeter fence gate. A closed circuit T.V. system shall be erected to allow remote assessment of personnel requesting access. A fixed duress alarm shall be positioned near the CCTV screen.

e. A procedure shall be established to provide for emergency call-back/notification. This procedure shall require the preparation of an emergency notification roster. The roster shall contain the names and telephone numbers of all persons of authority and other personnel deemed mission essential for emergency reaction.

f. Only authorized and official vehicles shall be allowed on site. Personnel parking shall be maintained outside the perimeter fence according to the requirements specified in paragraph 5.1.3.2.1.2.

5.1.3.3.2.3 Emergency Entry. In an emergency, firefighting, medical or other required emergency personnel shall be permitted entry to a site without delay. Said emergency personnel shall be kept under escort and surveillance by site operational or security personnel at all times and shall be restricted to the area containing the emergency situation.

5.1.3.3.3 Warning Signs. Restricted area signs shall be posted on all sites subject to the jurisdiction or administration of, or in the custody of the DoD or military departments of the DoD according to the requirements of DoD Directive 5200.8 and Section 21 of the Internal Security Act of 1950. Any posted sign shall not reveal the nature of the operation of the site and shall not present information about site personnel. Specific wording on signs shall be consistent with host nation requirements and posted in both English and local languages. Specifications for signs are presented in Figure 8. An example of a restricted area sign is also presented.

5.1.3.3.4 Cleared Area. An extended clear area of at least 9 m in width shall be maintained inside the perimeter fence through the use of chemicals or by routine ground maintenance. The cleared area shall have no obstacles, topographical features or vegetation greater than 20 cm in height.

5.1.3.3.5 Locks and Keys. All gates, manholes, cable vaults and doors shall be locked with high security key operated padlocks that meet or exceed the requirements of MIL-P-43607E. Key control procedures shall

be adopted that consist of step-by-step instructions to be carried out for issuing and maintaining keys. As a minimum, these instructions shall include the following steps:

a. A key control officer shall be appointed to have overall responsibility for issuance and maintenance of keys and locks.

b. Keys shall be accessible only to those persons whose official duties require access to them. A record shall be kept of the total number of keys and the names of persons to whom keys have been issued.

c. Padlocks shall be changed on a regular basis, whenever a key is lost, unaccounted for, or individual(s) has been transferred, taking a key with them, or when the current key control system has been subjected to compromise.

d. Keys shall be stored in a locked container when not in use. Access lists for those authorized to draw keys shall be kept in the same container.

e. Keys shall not be issued for personal retention, or for casual access during non-duty hours.

5.1.3.3.6 Sensors. One or more intrusion sensors shall be installed within Zone 1 for the purpose of detecting unauthorized penetrations into manned and unmanned facilities. Sensors shall be installed within the perimeter fence. For unmanned facilities, the sensor output shall trigger an audible alarm on site as well as in the facilities charged with alarm assessment and response force dispatch for that site. For these

sites, the alarm shall not be deactivated at any time. At manned facilities the sensor output shall trigger an audible alarm on-site only. The alarm shall not be deactivated unless the perimeter fence gate is opened to accommodate heavy traffic (see paragraph 5.1.3.3.1.3).

5.1.3.3.6.1 Factors Influencing Choice of Sensors. No single sensor is available that detects all possible methods of intrusion into Zone 1 and has an acceptable false alarm rate for the variety of site conditions found at DCS sites. Two or more sensors may be required to achieve a desired detection capability along with an acceptable false alarm rate. Each DCS site is unique in terms of the characteristics which influence the choice of exterior intrusions sensors. There is no single or combination of sensors that is applicable to all DCS sites. The choice of sensors shall be made after establishing the detection objectives of the Zone 1 sensors and assessing all of the factors that can influence the decision (Table 7). Assistance in the final choice and installation of Zone 1 sensors shall be obtained from the U.S. Air Force Physical Security Systems Directorate, Hanscom Field, Bedford, Massachusetts.

Since some of the sensors are still under development for military use, the annunciator/display systems to be used for specific sensor application can be determined through the security equipment supply office, or through coordination with the Project Office for Physical Security Equipment.

5.1.3.3.6.2 Applicable Sensors. Based on the typical operating environment of manned and unmanned DCS sites, sensors applicable to Zone 1 were rank ordered in terms of their applicability (Table 8).

Figures 9-12 present implementation details for the four highest ranked sensors. These details are presented solely to familiarize the user of this standard with the complexities of these devices.

5.1.3.3.7 Alarm Assessment and Procedures. An alarm triggered by a zone 1 sensor indicates the presence of one or more intruders inside the perimeter fence. The intruders' presence will be either authorized and, hence, predicted according to the site entry procedures specified in paragraph 5.1.3.3.2 or it will be unauthorized. For unmanned DCS facilities, assessment of the intrusion shall be made via two way audio equipment, the output of which is carried via voice grade channel to the site charged with alarm assessment and response force dispatch. Once an intrusion is verified, the response force shall be dispatched and a verbal challenge offered over the audio assessment system. At manned facilities, prompt visual assessment shall be made via CCTV. Once an intrusion is verified, the response force shall be dispatched.

5.1.3.3.8 Cables. All cables within zone 1 shall be buried according to the requirements specified in paragraph 5.1.3.2.5.

5.1.3.4 Zone 2 Security Measures. Security measures in Zone 2 are installed to provide intrusion deterrence and intrusion detection, to enhance alarm assessment and to protect critical equipments against standoff weapons fire.

5.1.3.4.1 Inner Fence. All DCS sites shall be surrounded by a continuous inner fence as specified in Figure 13. The inner fence shall be located no less than 9 m from the perimeter fence. The inner fence shall be located no less than 3 m from trees, poles, buildings, or any other potential climbing aids that are inside the inner fence.

5.1.3.4.1.1 Drainage. Drainage shall be provided to prevent standing water from accumulating near the inner fence. Specifications for drain lines and culverts shall be in accordance with paragraph 5.1.3.3.1.1.

5.1.3.4.1.2 Gates. Vehicle and personnel gates shall be constructed as specified in Figure 14. The number and location of gates shall be the same as specified in paragraph 5.1.3.3.1.3. (perimeter fence gates). Gates not under security force observation shall be securable to the strength of the adjacent fence construction and shall be locked. All gates shall be equipped with taut wire sensors.

5.1.3.4.1.3 Entrance. Entrance shall be in accordance with specifications in paragraph 5.1.3.3.1.4.

5.1.3.4.1.4 Gatehouse. For those sites where a guard is posted at an entry gate, a gatehouse shall be located within the inner fence and adjacent to its path of entry. Gatehouses shall be constructed as specified in Figure 15.

5.1.3.4.1.5 Entry Point Lighting. Entry point lighting shall be provided in accordance with specifications in paragraph 5.1.3.3.1.6.

5.1.3.4.1.6 Site Entry Control. Site entry control for unmanned and manned DCS sites shall be accomplished using the site entry control procedures specified in paragraphs 5.1.3.3.2, 5.1.3.3.2.1, and 5.1.3.3.2.2.

5.1.3.4.2 Sensors. The sensor in Zone 2 shall be a taut wire sensor installed as an integral part of the inner fence and gates. For unmanned facilities, the sensor output shall trigger an audible alarm on site as well as in the facilities charged with alarm assessment and response force dispatch for the site. At unmanned sites, the alarm shall not be

deactivated at any time. At manned facilities, the sensor output shall trigger an audible alarm on-site only. The alarm shall not be deactivated unless the inner fence gate is opened to accommodate heavy traffic and (see paragraph 5.1.3.3.1.3) a guard is posted at the gate.

5.1.3.4.3 Alarm Assessment and Procedures. Alarm assessment procedures shall be employed to verify a sensed intrusion. Specific procedures shall be adopted for dispatch of an appropriate response force when assessment indicates the presence of an intruder.

5.1.3.4.3.1 Unmanned Sites. Alarm assessment for unmanned DCS sites shall be accomplished by applying coincidence techniques to the sensors in Zones 1 and 2. An intrusion is verified when sensors in Zones 1 and 2 indicate an alarm condition within a time interval that is determined by the location of the sensors. When this condition exists, a response force shall be dispatched immediately to the site. When a single sensor indicates an alarm condition, the equipment building and tower shall be monitored acoustically in real time for 15 minutes to ensure that an intruder has not penetrated the other sensor line(s) without causing an alarm. If acoustic monitoring indicates an attempted or actual intrusion, a response force shall be dispatched immediately.

5.1.3.4.3.2 Manned Sites. Alarm assessment for manned DCS sites shall be accomplished visually through the use of video cameras as specified in Figure 16, the use of a manned guard tower as shown in Figure 17, or the appropriate combination thereof. Every sensor alarm shall be followed immediately by visual inspection of the area where the alarm was triggered. A visually confirmed intrusion shall be followed by immediate deployment of the on-site guard force and dispatch of the off-site response force.

5.1.3.4.4. Non-critical Buildings. All non-critical buildings, such as maintenance sheds, shall be removed from the site compound to facilitate visual assessment of the site perimeter and compound.

5.1.3.4.5 Fuel Storage Protection. Fuel storage tanks shall be buried where possible. If fuel storage tanks cannot be buried they shall be covered with a minimum of .5 m of overburden.

5.1.3.4.6 Lighting. Lighting in Zone 2 shall be employed to illuminate the site perimeter, inner areas, and entry points as specified in Figure 18. Lighting shall be located such that it does not interfere with CCTV or response force vision and does not highlight site personnel. The lighting system shall produce full lumen output within five seconds after it is energized. The lighting system shall have instant restart capability and produce full lumen output within five seconds after interrupted power is restored. Failure of one or more lights in the system shall not affect the operation of the remaining lights.

5.1.3.4.7 Gabion. All buildings on unmanned DCS sites shall be surrounded by a gabion as specified in Figure 19 to afford protection from standoff weapons fire. The gabion in this case is constructed to function as a revetment.

5.1.3.4.8 Cables. All cables within zone 2 shall be buried according to the requirements specified in paragraph 5.1.3.2.5.

5.1.3.4.9 On-Site Guard Force Procedures. For sites employing on-site guards, the operating command shall develop and implement specific procedures detailing on-site guard force responsibilities for alarm assessment, initial alarm response, perimeter patrol, security measure

inspection and assessment, entry control, key and lock control, and weapons control. These responsibilities shall be incorporated into existing guard orders and become a standard operating procedure (SOP) for the guard force.

5.1.3.4.9.1 Alarm Assessment Procedures. Upon the activation of a perimeter sensor, guard force personnel posted in a guard tower or at a CCTV monitor station shall visually assess the alarm. A verified intrusion shall result in immediate notification of the appropriate response force and immediate sounding of the DCS site's intrusion alarms. The guard force shall then man firing positions to provide the initial response and defense of the site.

5.1.3.4.9.2 Patrol Procedures. The guard force shall conduct 2 man patrols at random intervals to provide an intrusion deterrent and to inspect security measures such as fences, locks, doors, lights, etc. for degradation. The patrol route shall be varied between patrols. Vehicular patrols may be used on large DCS sites, however a foot patrol shall be conducted at least once daily to inspect the perimeter and inner fences. Patrols shall be armed and carry two way radios in order to maintain communications with site personnel. Night patrols shall avoid areas where they are highlighted by site lighting.

5.1.3.4.9.3 Site Entry Control Procedures. Site entry at manned DCS sites shall be controlled by a member of the guard force posted at a gate house or at a CCTV monitor. Procedures for site entry control shall be as specified in paragraph 5.1.3.3.2.2.

5.1.3.4.9.4 Key Control. Key control procedures shall be implemented by an on-duty member of the guard force designated as key control officer. Procedures for key control shall be as specified in paragraph 5.1.3.3.5.

5.1.3.4.9.5 Weapons Issue and Control Procedures. All members of the guard force shall wear sidearms while on duty. Other weapons and ammuni- tion shall be stored in approved storage containers which are locked and alarmed. All site personnel shall be issued keys to the weapons lockers when on duty to ensure speedy access to weapons in the event of an armed attack. One member of the guard force shall be designated weapons con- trol officer. The weapons control officer shall be responsible for the security, maintenance, and issue of weapons and also for the training of site personnel in proper weapons use.

The using activity will designate certain members of the operational staff to provide support to the guard force during emergencies. These personnel shall be trained and certified competent in the use of firearms to include the shotgun, rifles, and handguns of the type which are standard issue for the protection of DCS sites. Competency should be certified by the military or local police.

There shall be stored at the site sufficient numbers of these weapons and a sufficient supply of ammunition for each weapon to ensure reasonable support for the guard force.

5.1.3.5 Zone 3 Security Measures. Security measures are installed in Zone 3 to provide detection and intrusion delay. Some measures also provide improved resistance to damage of site components.

5.1.3.5.1 Critical Buildings. All essential equipments and power sources shall be housed in buildings. Existing sites shall utilize in place structures to the maximum extent possible. Existing buildings shall be modified in accordance with paragraphs 5.1.3.5.3, 5.1.3.5.5 and 5.1.3.5.6. Existing unmanned sites that utilize trailers, vans or portable vaults to shelter essential equipments and power sources shall contain said shelters in vaults that are constructed in accordance with Figure 30. New unmanned DCS facilities shall be constructed in accordance with the specifications in Figure 20.

5.1.3.5.2 Tower Barriers. All antenna towers and free standing antennas on new and existing unmanned DCS sites shall be contained in vaults as specified in Figure 21. At manned DCS sites, a fence, as specified in Figure 6 shall be built around antenna tower bases and free standing antennas.

5.1.3.5.3 Obscurants. All critical buildings and tower vaults on unmanned DCS sites shall contain smoke generators as specified in Figure 22. The smoke generators shall be activated by remote control from the facility charged with the responsibility for sensor monitoring, alarm assessment, and dispatching the response force. The smoke generators shall be equipped with a fail-safe mechanism to prevent activation when authorized personnel are in the building.

5.1.3.5.4 Building Entry Control. Entry control into buildings on DCS sites shall be in accordance with specifications in paragraphs 5.1.3.3.2, 5.1.3.3.2.1 and 5.1.3.3.2.2. Entry control procedures for access into buildings on manned DCS sites shall include the following guidelines:

a. All doors shall be kept locked.

b. Upon entering the site, authorized personnel shall be issued appropriate door keys and weapons storage keys by the key control officer.

c. Upon leaving the site, personnel shall surrender said keys to the key control officer.

5.1.3.5.5 Protection for Doors, Windows, and Other Openings. Doors at DCS sites shall be constructed in accordance with specifications in Figure 23. A panic bar shall be installed on the inside of the door. Windows at all DCS sites shall be protected in accordance with specifications in Figure 24. Openings in building walls greater than $624cm^2$ in area and with a smallest dimension greater than 16cm shall be covered by a welded iron grid. All nonessential openings shall be covered with armorplate in accordance with Figure 24 of this standard.

5.1.3.5.6 Sensors. All doors at unmanned DCS sites and the doors to weapons storage lockers at manned facilities shall be equipped with balanced magnetic switch sensors specified in Figure 25. All critical buildings and tower vaults at unmanned DCS sites shall be equipped with interior microphones as specified in Figure 26.

5.1.3.5.7 Alarm Assessment and Procedures. Upon reception of an alarm initiated by a perimeter sensor at unmanned DCS sites, tower vaults and equipment buildings shall be monitored acoustically through the microphone sensors specified in paragraph 5.1.3.5.6. If an attempted or actual penetration is sensed through the microphone sensors or through balanced magnetic door switches, the smoke generators specified in paragraph 5.1.3.5.3 shall be activated and the appropriate response force dispatched.

5.1.3.5.8 Antenna Protection. All antennas or antenna feeds located on DCS sites shall be protected by radomes or other suitable structures as specified in Figure 27. These radomes and structures should provide a visual obstacle to prevent small arms attacks on the antenna feed system. Depending upon antenna type and size, it may be appropriate to protect the whole antenna.

5.1.3.5.9 Waveguide Protection. All exterior waveguide runs shall be located no less than 4m above ground level. All waveguides shall be armored in accordance with specifications in Figure 28 to protect against damage from penetration tools and small arms fire.

5.1.3.5.10 Guy Wire Protection. All guy wires and anchor points shall be protected by sleeves and vaults as specified in Figure 29. All anchor points outside the inner fence shall be treated as separate unmanned facilities and the appropriate security measures specified in paragraphs 5.1.3.2 through 5.1.3.6 shall be applied.

5.1.3.5.11 Air Conditioning. All air conditioning units essential to the operation of the communications equipment shall be moved to a minimum of 4 m above ground or to the roof of the building.

5.1.3.6 Zone 4 Security Measures. Security measures are installed in Zone 4 to provide intrusion delay.

5.1.3.6.1 Protection of Critical Equipment. All essential equipments and power sources within buildings at unmanned DCS sites shall be consolidated and then housed in vaults according to specifications in Figure 30. Only equipment necessary to the communications function of the site shall be afforded this protection. Existing trailers, vans or

portable vaults may be substituted for the equipment vault as long as these structures are contained within a building.

5.1.3.6.2 Tower Leg Protection. All tower legs at manned and unmanned DCS sites shall be protected according to specifications in Figure 31.

5.1.3.6.3 Guy Wire Anchors. All guy wire anchors shall be encased in sleeves as specified in Figure 29.

5.1.3.7 Vulnerabilities-Security Measures Matrix. The vulnerability-security measures matrix, Table 9, is a security planning tool for correlating site vulnerabilities, identified in accordance with the procedures detailed in paragraph 5.1.2, with security measures which have an impact on specific vulnerabilities. The vulnerability-security measures matrix is given in Table 9. The upper row lists site vulnerabilities that have been found at typical DCS facilities. The lower row of the vulnerability-security measures matrix contains the security measures applicable to each vulnerability in the form of an alphabet code. The key to the code is given in Table 10 in terms of paragraphs contained in this standard which describe the implementation of the appropriate security measures. The matrix is divided into zones. Blank columns are provided to allow the security planner to add additional vulnerabilities and appropriate security measures based upon a survey of each specific site.

A vulnerabilities-security measures matrix should be prepared by the security planner to identify the security measure systems that may be available to deal with an identified vulnerability. All security measures which could impact on a given vulnerability should be identified as

candidate measures. The resulting matrix will then contribute to a "catalog" of available measures, which used singly or in combination, to mitigate a given vulnerability.

5.1.4 Effectiveness of Security Measures

5.1.4.1 Protection-Allocation Matrix. The specific security measures to be implemented at a given site shall be selected based upon those identified as candidate security measures in the vulnerabilities-security measures matrix, Section 5.1.3.7. Having completed the identification of the available security measures, the next step is to evaluate the relative effectiveness of the available securty measures systems. To accomplish this task a protection-allocation matrix shall be prepared. The protection-allocation matrix correlates the identified site vulnerabilities with the available countermeasures. The elements of the matrix are qualitative or quantitative statements of the effectiveness of the countermeasures in meeting site endurability requirements. An example of a protection allocation matrix is given in Table 11.

In preparing a protection allocation matrix the site security planners must recognize that a security measure found effective at one site may not be as equally effective at another site. Thus, a protection allocation matrix shall be tailored for each site.

5.1.4.2 Use of Protection Allocation Matrix. The protection allocation matrix is used for two purposes: 1) to express in qualitative and quantitative terms the degree of protection required for the various subsystems in order to meet the required site endurability objectives; 2) to express the degree of protection achieved through the use of selected countermeasures.

In planning the security measures for a particular site, the security planner inserts the required effectiveness of a given measure in the elements of the matrix. In the effectiveness allocation process, the planner must keep in mind that some countermeasures reinforce or contribute to the effectiveness of other countermeasures.

After completing the protection allocation matrix displaying required effectiveness, the security planner develops a second protection allocation matrix on which the elements display the achieved level of protection provided by the individual or combined security measures. The data describing the effectiveness of various countermeasures and countermeasures combinations may be obtained from such references as the "Barrier Technology Handbook," from support engineer organizations, from security equipment development agencies, and from special operations personnel.

In practice, the security planner may iterate the process of developing the protection allocation matrix until the achievable level of protection compares favorably with the required level of protection.

Table 11 presents an example of protection allocation matrix prepared for an unmanned mircrowave repeater site against which the maximum threat is determined to be a casual vandal. On the basis of low criticality of the site in the DCS network, the security planner has determined that the objective of the security measures to be installed is to deter vandals and limit the areas to which a vandal would have easy access.

Across the top of the matrix are listed the vulnerabilities that a vandal could exploit if no security measures had been installed. On the left side of the matrix are the security measures chosen for implementation at this particular site.

Power and communications cables are to be buried per instructions in section 5.1.3.2.5 of the standard. Fences and lights are to be installed in Zones 1 and 2 according to criteria in sections 5.1.3.3 and 5.1.3.4. To remove the vulnerability of exposed fuel tanks, the tank will be buried as described in section 5.1.3.4.5. To reduce the likelihood of damage to air conditioning units, they are to be relocated to the roof of the communications building per section 5.1.3.4.10 and obscured by placing metal grating around the air conditioning units.

To prevent access by a vandal to the communications equipment and generators, the building door is to be upgraded to meet specifications in Figure 22 and the windows are to be covered according to specifications in Figure 23.

Waveguide external to the building is to be protected using techniques described in Figure 27.

5.1.4.3 Response Force Characteristics

5.1.4.3.1 Size. The response force shall consist of ten or more personnel, in addition to any personnel already on the site.

5.1.4.3.2 Capability. The response force shall be capable of responding to site penetrations and using armed force to prevent further damage or destruction of facilities after their arrival.

5.1.4.3.3 Response Time. The response time must be less than the amount of time required by adversaries to accomplish major damage to critical items at the site. Response time must ensure achievement of this objective but in no case exceed 15 minutes.

5.1.4.3.4 Weapons. The response force shall be equipped and armed for combat type operations as determined appropriate by the commander responsible to provide the force, in coordination with the commander of

the site to be supported. The local surrounding environment shall be considered in authorizing the types of weapons to be employed. The below listed weapons or comparable types, shall be considered for use.

a. 12 guage shotgun

b. M-16 rifle

c. M-60 machine gun

d. 40mm grenade launcher

e. .38 caliber pistol

f. .45 caliber pistol.

5.1.4.3.5 Equipment. Response force personnel shall be equipped with protective masks, flak vests and helmets. This equipment, plus the issued weapons and appropriate ammunition, shall be kept at a designated location in the unit area, ready for immediate response force departure. The response force shall also have wire cutters or bolt cutters in case fence cutting is necessary to accomplish their mission. The vehicle(s) necessary to transport the response force to the site shall meet high standards of reliability. They shall be kept near the response force arms and equipment and shall be used for no purpose other than transporting the response force.

5.1.4.3.6 Organization. The commander responsible for providing response force support to the site shall organize the force as deemed appropriate to accomplish the mission. Response forces shall be available on a 7-day, 24-hour basis. Written orders shall be issued to all personnel identified for this mission.

5.1.4.3.7 Training. Personnel assigned response force duty shall receive an orientation briefing, including a visit to the site, on their first shift of such duty. Response force exercises, simulating actual emergencies, shall be held at least once each month. Half of these exercises shall be held during the hours of darkness.

5.2 Unique Site Protection

5.2.1 Classification of Sites as Unique

The security measures specified in Section 5.1 above have been formulated upon the assumption that the security manager has sufficient space onsite to implement the indicated security measures, and that the manager has full authority to implement the indicated security measures.

There are, however, numerous DCS sites which provide unique challenges to the security manager in the planning and execution of security measures. This section describes some approaches to dealing with unique sites.

Any one of the following factors may be reason for a site to be classified as being unique in regard to security measure implementation:

- Site size
- Colocation with other activities
- Proximity to uncontrollable terrain or space
- Soil conditions
- Unique site components.

Site size renders a site unique if the site is so small that a multiple zone approach to deterrence, detection, and delay is infeasible, or so large that incorporation of the whole site in a multiple zone defense is impractical operationally or costwise.

Colocation with other activities renders a site unique if the responsibility for security within the site becomes ambiguous or impossible to enforce in areas required for adequate security measures. This may be the case when site users include commercial users or foreign nationals.

Proximity to uncontrollable terrain occurs when the site's critical assets are located adjacent to public access thoroughfares, other buildings, or terrain. DCS sites located in buildings contiguous to walkways, and highways often leave no barrier, except a single wall, between critical assets and a potential adversary. As a site qualification factor, proximity to uncontrollable terrain is often combined with site's size, resulting in a severely limited set of applicable physical security measures.

Soil conditions may make the installation of sensors difficult or impractical, or may limit the kinds of construction feasible on a given site. Permafrost areas or marsh areas could limit fence line or wall construction and sensor emplacement

Unique site equipments, e.g., antenna arrays, may render a site unique when critical site components cannot be protected using the security measures identified in the standard.

5.2.2 Threat Analysis Threat analysis for unique sites proceeds upon the same lines as that for generic sites. Through consultation with intelligence support agencies and local security forces, and using available operation experience those individuals and groups posing a threat to a site are identified.

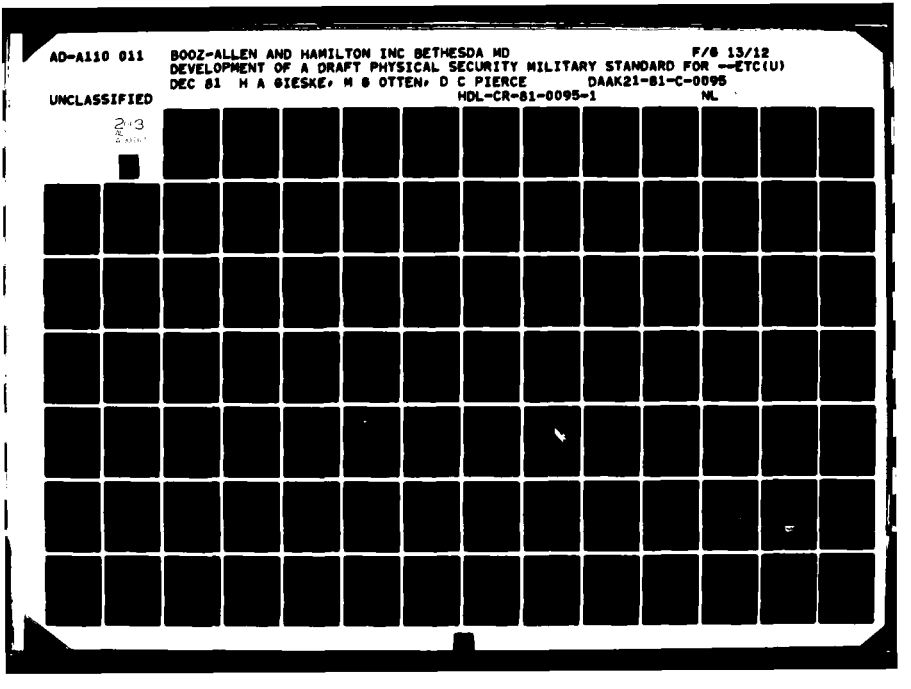
In analyzing the threat to a unique site, it is important to analyze whether the site's unique characteristics may be exploited by the threat. For instance, a site having a wall adjacent to a public thoroughfare may provide a way for an adversary to place extraordinary amounts of explosives adjacent to a DCS facility without crossing an intrusion sensor. A different situation occurs when a site is located in such a place that it would be extraordinarily difficult for an adversary to carry significant quantities of explosives. This latter case might be a DCS facility located inside a well protected, blast hardened building.

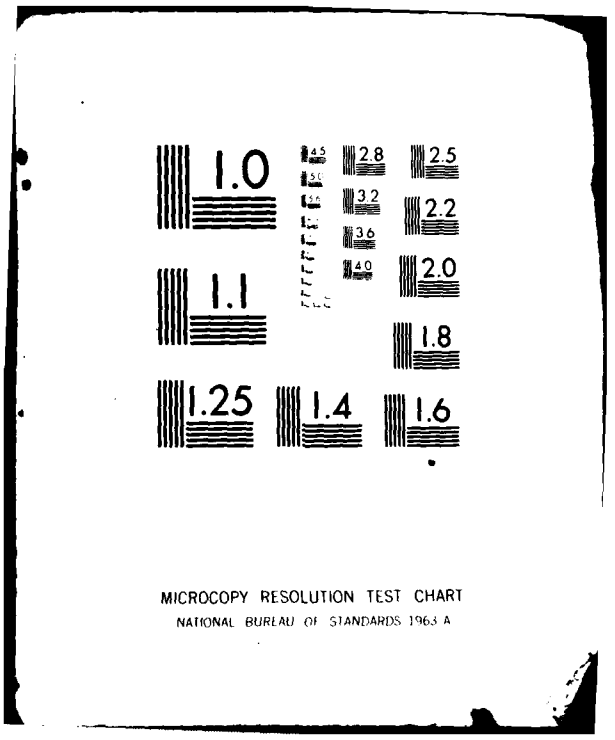
In conducting a threat analysis for a unique site, the security planner shall identify all those site features which cause the site to be classified as unique and shall describe how each of the factors may be exploited by an adversary to enhance adversary capability. Unique site factors that affect site security will be considered in Section 5.2.4 below.

5.2.3 Unique Site Susceptibilities. Susceptibilities found on unique sites may be the same as those found on a generic site or they may be strictly unique. As indicated above, unique equipment may render a site unique. If the unique equipment has an unusual sensitivity to damage or disruption, the unique equipment shall be classified as a unique susceptibility. In analyzing the susceptibilities on a unique site the security planner shall list the unique equipment among the site susceptibilities. It is particularly important to indicate the susceptibilities that an adversary might exploit. Table 12 lists some unique site characteristics and related susceptibilities.

5.2.3.1 Unique Site Susceptibility Surveys. The security planner will need to carefully evaluate and analyze the findings of site surveys to determine the most cost effective approach to providing security.

There may exist in some unique sites, situations which are beyond the control of the planner but still present serious security problems. For example, sharing the facility with foreign nationals may limit personnel identification. Not being able to remove dense unwanted shrubbery, due to local or national ordinances, may result in poor visibility. Location close to radar emissions sources, such as from an airport, may complicate the choice and installation of sensors. It may be in the best interest of the overall mission to consider the feasibility of relocating the site to a more ideal location. Mission criticality shall be a key factor in making such a decision to relocate.


AD-A110 011
BOOZ-ALLEN AND HAMILTON INC BETHESDA MD
F/6 13/12
DEVELOPMENT OF A DRAFT PHYSICAL SECURITY MILITARY STANDARD FOR --ETC(U)
DEC 81 H A GIESKE, M G OTTEN, D C PIERCE
DAAK21-81-C-0095
UNCLASSIFIED
HDL-CR-81-0095-1
NL
2 3


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963 A

(Left blank intentionally)

5.2.4 Unique Site Security Measures. It is not within the scope of this military standard to provide specific security measures for each unique site vulnerability. Rather the purpose of this section is to identify recommended approaches to be considered by the security planner in dealing with unique security situations, to achieve deterrence, detection, delay and denial. In planning unique site security measures the security planner shall first consider the security measures given in section 5.1.3 for generic sites. When security measures identified in section 5.1.3 cannot be implemented for technical or practical reasons, the planner should in addition consider the security measures discussed here.

5.2.4.1 Unique Site Zone 0 Security Measures

5.2.4.1.1 Very Large Sites. If a site is unique because of its very large area, resulting in poor observation over the site, a fence on the outer boundary may provide no useful intrusion deterrence or detection. Under these circumstances the security planner shall consider the site as unprotected and identify site assets that require zonal security measures. In identifying site assets the security planner shall consider subdividing the large site into sub-sites that may be be treated as manned or unmanned facilities to which the security measures of section 3.1.3 may be applied on a sub-site by sub-site basis. Subdivision of a very large site into sub-sites will simplify total site security planning, and conserve resources to protect the most vital assets. The security planner shall use as guidance the principle that the security program is to protect capabilities and not terrain.

5.2.4.1.2 Small Sites. Ordinarily a very small site does not have the space to accommodate Zone 0 security measures which are ordinarily

installed to deter vehicular intrusion. Consideration should be given to locating vehicle entrances so that straight line approaches by vehicles do not end at critical facility components.

Where possible vehicle barriers such as described in figure 3 should be placed along the outer fence line, adjacent to roadways, to prevent damage or penetration of the outer fence by vehicles.

Additional consideration should be given to the feasibility of building a reinforced concrete wall around the site. This would help prevent the use of vehicles in damaging the site and its outside equipment.

5.2.4.1.3 Soil Conditions. Soil conditions may prohibit the installation of vehicle detection and deterrence measures. Nonetheless, all access roads should be configured and/or lined, as in section 5.1.3.2.1.1 to channel vehicles along specified routes of approach. Where soil conditions are such that buried cable vehicle sensors are not feasible, consideration should be given to the use of radar sensors to detect vehicular traffic. Alarm assessment procedures shall be the same as described in section 5.1.3.2.3.

5.2.4.2 Unique Site Zone 1 Security Measures.

5.2.4.2.1 Very Large Sites. After a very large site has been subdivided into subsites, the security measures given in section 5.1.3.3 shall be applied.

5.2.4.2.2 Small Sites. Generally speaking, the security measures identified in section 5.1.3.3 shall be applied to small sites. The situations where the standards for the perimeter fence locations cannot be

applied, the security planner should ascertain if barbed tape or other deterrents to climbing can be applied to poles, building roof lines, or other paths and points of site ingress.

5.2.4.2.3 Colocation With Other Activities. When a DCS site is colocated with other activities, implementation of Zone 1 security measures shall be coordinated with the other activities. Joint access rosters shall be maintained and regularly updated to control access to both manned and unmanned sites. Entry control procedures as given in 5.1.3.3.2 shall be established in coordination with the other colocated activities. When security measures standards of the various colocated activities differ, this standard or more stringent standards shall apply.

5.2.4.3 Zone 2 Security Measures for Unique Sites.

5.2.4.3.1 Small Sites. When sites are so small that an inner fence is not feasible, intrusion sensors shall be applied to potential building or vault entry points per section 5.1.3.5.6. For unmanned sites the sensor output shall trigger an audible alarm on site as well as in facilities charged with alarm assessment and response force dispatch. At unmanned sites the alarm shall not be deactivated at any time. At manned facilities the sensor output shall trigger an audible alarm on site only. Alarm assessment procedures shall be as provided in 5.1.3.4.3.

5.2.4.4 Zone 3 Security Measures in Unique Sites. As with generic sites, Zone 3 security measures are installed to provide intrusion delay or improved resistance to damage of site equipments. Where feasible the security measures given in section 5.1.3.5 should be applied. Below are some recommended approaches to specific Zone 3 problems.

5.2.4.4.1 Building Entry Control. Building entry control, for small sites, colocated sites, or those in proximity to uncontrollable space, may require modification based upon the lack or inadequate effectiveness of Zone 2 controls. Additional personnel entry control and intrusion delay may be obtained by installing an intrusion resistant vestibule, Figure 32, at personnel entry points. The vestibule doors shall be interlocked so that both doors may not be open simultaneously and the size of the vestibule shall be no larger than that required for one person to open the inner door. At manned sites entry through the vestibule will be controlled by personnel inside the facility by use of an electronic striker and lock. Observation of personnel in the vestibule will be accomplished through one-way viewing or closed circuit television system. One-way viewing system shall be installed to prevent an intruder from threatening personnel on the inside of the facility.

5.2.4.4.2 Large Antenna Arrays. Low frequency or troposcatter antennas may constitute a unique protection problem. All large antennas shall be assessed to identify the location of critical antenna feed points and the impact of the loss of antenna elements.

Large distributed antennas shall be fenced, compatible with antennas performance requirements. The terrain around such antennas shall be graded and/or barricaded to deter the use of vehicles in the rapid destruction of large arrays.

Tropospheric scatter system antennas (feedhorn and reflector) shall be treated as two separate components requiring protection measure analysis. Feedhorn and waveguide protection shall include use of measures given in 5.1.3.5.8 and 5.1.3.5.9.

5.2.4.5 Zone 4 Security Measures for Unique Sites. Zone 4 measures are implemented to provide a second level of intrusion delay and equipment damage mitigation. Site size, colocation and proximity to uncontrolled space may impact the feasibility of constructing equipment vaults according to section 5.1.3.6.1. As a minimum protection against the effects of blast and collapse of exterior walls, critical equipment shall be located as far from exterior walls as possible. Where floor loading and space permits a blast and fragment suppression curtain shall be installed near exterior walls as indicated in Figure 33.

5.3 Security Program Plan. The operating activity shall be responsible for establishing, planning, organizing and implementing an effective security program at each DCS site. A formal document describing the planned implementation shall be developed for each site. The plan, a topical outline for which is given in Appendix A, shall include, as a minimum, the elements described in sections 5.3.1 through 5.3.10. The Security Program Plan is a first level planning document used to bring into coordinated focus all the considerations that may be pertinent to planning security for a given site. The program plan deals with the management aspects of site security planning including systematic consideration of threat, site missions, measures available, functions of specific organizations, and the budget and programming process. The security program plan is distinguished from the Site Security Plan, section 5.3.10.1, which is the detailed plan for actual installation, and/or operation of site security measures.

5.3.1 Threat Analysis. The operating activity shall determine, in combination with the appropriate military department counterintelligence/ investigative activity which is responsible for the geographical area of

the site concerned, the nature and capabilities of the threat to the site. Preparation of the analysis by the appropriate military department counterintelligence/investigative organization will ensure strict compliance with the provisions of DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense," January 7, 1980, and military department implementing regulations.

The threat against a specific DCS site depends upon the geographical location of the site, the political, social and economic environment in the area, the function of the site, and the goals of potential adversaries, as well as other factors. The threat analysis shall identify, in as much detail as necessary, the identification of persons, groups, organizations and foreign agents who constitute a possible threat to the site. The analysis shall include the threat posed by vandals, political demonstrators, terrorists and saboteurs, and shall consider periods of peacetime and pre-hostility tension, conventional war, limited nuclear war and general nuclear war. The analysis shall contain enough detail on threat organization, training, equipment and motivation to permit an evaluation of the probable effectiveness of candidate security measures. The threat analysis shall be updated at least annually, or more frequently if warranted by changing conditions.

5.3.2 Site Susceptibility Analysis. Site susceptibilities are the specific site elements, e.g., power lines and waveguides, that are essential to site operation and whose damage or destruction would eventually cause loss of facility function. Each DCS facility requires the continuous function of specific operations such as power generation or conversion, signal transmission and reception and data processing to accomplish

its mission. Disruption or loss of a single such operation leads to the ultimate loss of capability and mission failure of the site. Fault tree analysis shall be applied to site operational flow diagrams to identify the failure modes of the site. The identified failure modes shall be compared with the actual physical layout and integration of the site (or site plans for a new site) to arrive at site susceptibilities.

5.3.3 Vulnerability Analysis. The vulnerability analysis is used to correlate the identified threats (5.3.1) with specific site susceptibilities (5.3.2) to produce the Threat Vulnerability Matrix. Site susceptibilities, as they apply to each security zone, shall be arrayed across the top of the matrix. Some susceptibilities, such as power lines and communications cables, will appear in more than one security zone. All threat categories applicable to the site shall be arrayed down the left side of the matrix. The security planner shall then evaluate each column-row corbination and mark those boxes which indicate a susceptibility which may be exploited by the identified threat element. When this process is complete, the Threat Vulnerability Matrix will identify specific site vulnerabilities which require physical security protection.

5.3.4 Criticality Analysis. Each individual site within the DCS performs a different mission. This mission varies depending upon the location, the subscribers served, the scenario, the communication media utilized and the degree of redundancy in the network. The operating activity, in coordination with the Defense Communications Agency, shall perform a mission analysis to evaluate the criticality of the specific site, as related to others in the DCS. The statement of site criticality thus developed, shall be used to prioritize the allocation of physical security resources.

5.3.5 Endurability Analysis. The mission analysis performed in the Criticality Analysis (5.3.4) shall also be utilized to evaluate site endurability requirements. This analysis shall result in identification of the minimum amount of time which the specific site must remain operational under the most critical national and local conditions. The statement of site endurability shall be used to identify appropriate physical security measures for the site.

5.3.6 Security Measures Options. There are many different security measures available to apply against identified site vulnerabilities. Specific types of security measures which have been determined to be viable tools in solving DCS site vulnerability problems are included in Security Measure Implementation Instructions (5.1.3). The appropriate application of specific types of security measures against specific vulnerabilities is shown in the Vulnerabilities-Security Measures Matrix.

5.3.7 Security Effectiveness Analysis. Each Security Program Plan shall contain the criteria for evaluating the effectiveness of security measures which may be implemented. In general, the effectiveness of security measures shall be measured according to the degree of deterrence, the amount of delay or the degree of damage limitation resulting from use of the security measure. Security effectiveness criteria utilized by operating activities shall be coordinted with DCA so that, where appropriate, security measures will be evaluated under the same criteria for each site.

5.3.7.1 Deterrence Effectiveness. The deterrence value or effectiveness of a specific security measure or combination of measures is not quantifiable. However, experienced security managers can make judgments of the deterrence effectiveness of specific measures against certain

threats, e.g., vandals or demonstrators, on the basis of experience at similar sites or at other facilities utilizing similar measures. Where no experience base is available, security planners should assume that security measures provide no deterrence to a dedicated terrorist or saboteur.

5.3.7.2 Delay Effectiveness. The delay value or effectiveness of a specific security measure is quantified in terms of the additional time required for an intrusion or act of sabotage due to the presence or implementation of the security measure. The additional time may be due to the need for stealth, time needed to bypass or penetrate a barrier or time needed because additional equipment, weapons or explosives must be carried. Security planners should evaluate the effectiveness of security measures singly and in combinations to identify the maximum possible effectiveness expected for a given set of security measures.

5.3.7.3 Damage Limitation Effectiveness. The damage limitation value or effectiveness of a specific security measure can be measured in terms of additional tasks (including use of explosives) required to achieve a given level of damage or in terms of site elements that will have reduced damage as a result of implementing the security measure.

5.3.7.4 Response Time. Response time is measured from the time an alarm is assessed as requiring a response to the time required for the security response force to bring adequate force to bear upon intruders so that no further damage is done to the site. In evaluating security measure effectiveness (including the stationing of security forces), response time should be less than the delay time resulting from security measure implementation but in no case exceed 15 minutes.

5.3.8 Selection of Security Measures. The selection of specific security measures to be implemented shall be determined using the planning procedures described in section 5.1.4.1.

5.3.9 Implementation Plans. After the appropriate security measures have been selected and approved, the operating activity shall take action to implement the site security upgrade. This action shall be based upon implementation plans that specify actions to be accomplished by specific agencies, organizations, or commands.

5.3.9.1 Equipment Selection. In coordination with the Air Force Physical Security Systems Directorate, Hanscom AFB, MA (for exterior sensors and CCTV) and the Army Project Office for Physical Security Equipment, Ft. Belvoir, VA (for interior sensors, smoke obscurant systems and command control element), specific equipment items shall be selected. Arrangements shall be made for small scale on-site testing of selected exterior sensors to ensure that they will function under the environmental conditions existing at the site. Estimates shall be obtained on equipment costs, installation costs, operations costs and maintenance costs as well as operational staffing requirements and training requirements.

5.3.9.2 Planning, Programming and Budgeting. The operating activity shall take necessary actions to ensure that resources necessary to support the Security Program Plan are appropriately included and supported in their budget system. Equipment purchase and installation costs, operational staffing and training requirements, and operations and maintenance (O&M) costs must be determined and included in the Budget and Manpower Management Systems. Security measures requiring construction shall

be included in military construction budgets if major construction is required, or in other budgets for site upgrade or renovation. The overall implementation plan may be scheduled over a multi-year time frame to accommodate budget constraints.

5.3.9.3 Installation. The operating activity must plan carefully to ensure that the actual installation of security measures is done correctly. Extra care during this phase is more than offset by reduced O&M costs and more effective security throughout the life of the system. Continuous close supervision by knowledgeable personnel is required. If such personnel are not available, local personnel shall be selected and trained prior to installation of the system. Careful planning of the security system installation will also minimize disruption at existing sites and reduce delays at new sites. Commercial equipment firms may be invited to observe installation of their equipment in order to avoid mistakes and later operational problems (as well as make them more responsible for effective operation of their equipment).

5.3.9.4 Testing. As soon as installation of security modules (sensor systems, etc.) is complete, validation testing shall be accomplished. Validation testing shall be conducted in accordance with 5.4 Security Measure Effectiveness Tests.

5.3.10 Operations Evaluations. The operating activity shall take all necessary actions to ensure the continuity and effectiveness of the Site Security Program. Security operations evaluations are a key part of this effort and shall include the elements described in sections 5.3.10.1 through 5.3.10.3.

5.3.10.1 Site Security Plan. A Site Security Plan shall be developed and maintained, describing how security is provided to the DCS site. It shall describe the threat, security objectives and how these objectives are to be met. The plan shall be kept up-to-date and shall be a part of every site inspection. An outline of the security plan is include in Appendix B.

5.3.10.2 Equipment Tests.

5.3.10.2.1 Equipment Tests - Manned Sites. Daily checks shall be made of the perimeter fence, clear zones and lights to identify burned-out lights and evidence of undetected intruders. Spot checks of every segment of perimeter sensors shall be made weekly. Every door sensor shall be checked weekly. These tests shall be conducted in the same manner as validation tests (5.4.2). CCTV output shall be checked against the optimal video recording at least once each month. Equipment tests shall be logged.

5.3.10.2.2 Equipment Tests - Unmanned Sites. The perimeter fence, clear zone and lights shall be checked on a weekly basis to identify burned-out lights and evidence of undetected intruders. Spot checks of every segment of perimeter sensors and every door and audio sensor shall also be made on a weekly basis. These tests shall be conducted in the same manner as validation tests (5.4.2). Equipment tests shall be logged.

5.3.10.3 Response Force Tests. Announced Response Force tests, simulating actual emergencies, shall be conducted weekly at manned sites and monthly at unmanned sites. Half of these tests shall be held during the hours of darkness. For safety purposes care shall be taken to ensure that all personnel involved are informed that these exercises are not real emergencies.

5.4 Security Equipment Effectiveness Tests.

5.4.1 Objectives. There are two objectives of effectiveness tests. The first objective is to ascertain whether equipments proposed for installation at a new or existing site will perform to a satisfactory level at the site and under the expected environmental conditions. Experience has shown that security equipment in general does not necessarily perform to the same level of effectiveness in all applications. Therefore, effectiveness tests shall be conducted on proposed security equipment prior to its final selection as part of the overall site security program.

The second objective of equipment security tests is to ensure that security equipments have been properly installed and maintained.

5.4.2 Test Responsibilities. It shall be the responsibility of the operating activity to evaluate the effectiveness of proposed or installed security equipment. A Security Equipment Effectiveness Test Checklist is givin in Table 13 to assist in this requirement. Once system installation is complete, the operating activity shall conduct validation tests to ensure that the security system functions in accordance with its design. Where proper functioning requires actions by non-site personnel, the test should include all personnel or agencies involved or expected to respond to a security alarm.

5.4.3 Effectiveness Test Teams. In executing the responsibilities given in section 5.4.2, the operating activity shall establish a test team consisting of personnel familiar with the specific security equipment under test, and of personnel who have responsibilities to respond to security alarms. The test team shall accomplish the following:

- Prepare a plan to conduct effectiveness tests;
- Test and examine existing and proposed security equipments and their interface with other security program elements such as response forces;
- Provide a report to the security planner/manager detailing the test findings, and where possible, identify remedial actions for equipment performance deficiencies.

5.4.4 Maintenance and Inspection Testing. Inadequate maintenance of security equipment often results in equipment becomming ineffective, thereby leading to degradation of the overall security system. The operating activity shall periodically conduct inspections and maintenance testing to assure that maintenance procedures have been implemented and that equipment functions properly after maintenance activity has been performed. These maintenance test requirements may be made part of an overall security system effectiveness test activity.

Where necessary, individuals conducting the maintenance tests should establish a point(s) of contact for technical information concerning specific characteristics, operations, and maintenance requirements of the various security equipments installed on a given site. Points of contact can be developed from the facility engineers, the physical security development agencies, and equipment vendors.

5.4.5 Security Equipment Effectiveness Test Planning. A valid effectiveness test depends upon the preparation of a test plan which details the conditions for the test and the criteria for evaluating test results. An effectiveness test plan shall be prepared prior to the accomplishment of security equipment effectiveness testing. This plan shall include:

- Establishment of the test team and identification of its members
- Assignments of team responsibilities
- Review of current site security status to identify existing or suspected security system performance shortfalls
- Determination of test methods to be used and criteria for evaluating results
- Identification of actions to be taken based upon results of testing activity.

5.4.6 Equipment Effectiveness Rating. During the performance of the security equipment effectiveness test, the test team should provide the security planners with an effectiveness rating of the equipment. The rating will provide the planners with information concerning the suitability of equipment being tested or used at DCS sites. Table 14 can assist the test team in rating the security equipment.

5.4.7 Equipment Effectiveness Test Procedures. Systematic test procedures are required for consistent test planning and/or comparison of test results to determine trends in system performance. The following are test procedures for evaluating the applicability of a specific system at a new site or for evaluating systems already installed. The security system effectiveness planner shall prepare a test procedure for each of the security equipments to be tested. The test procedure given in sections 5.4.7.1 through 5.4.7.10 may be used as given or adapted to the specific equipment under test. In all cases the effectiveness test planners shall assure that the test procedure for a given system are capable

of demonstrating whether or not a system meets the performance requirements based upon its intended contribution to overall site security. The following test procedures are given below in single page form for easy reproduction if desired.

5.4.7.1

EQUIPMENT EFFECTIVENESS TEST PROCEDURES

Security Measure	Type of Test	Performance Indicator
Access Road Sensor	Technical Performance	Activate Alarm

Test Method: Vehicle Test

1. The vehicle test shall be conducted in a straight line in two directions on both sides of the road. Test speeds shall be 8, 16, and 65 km/hr.

   . Sensitivity or gain shall be set at the lowest level consistent with meeting performance requirements in order to reduce the possibility of unidentified alarms.

Note: Performance test shall be conducted while monitoring the output relay for the presence of an alarm condition.

Point of Contact:

5.4.7.2

EQUIPMENT EFFECTIVENESS TEST PROCEDURES

Security Measure	Type of Test	Performance Indicator
Ported Coax Cable Sensor (PCCS)	Technical Performance	Activate Alarm

Test Method: Walk Test

1. Lay a string or rope on the ground to indicate the cable location.

2. Test personnel shall walk at a normal rate perpendicular to the cable. The walk test shall be repeated at intervals of approximately one meter. Thus, 100 walks should be performed for each 100 meter segment.

Note: Performance test shall be conducted while monitoring the annunciator panel for the presence of an alarm condition. Initial tests shall be done under both normal and water saturated soil conditions.

Test Method: Run Test

1. Run tests shall be repeated at intervals of approximately three meters or less, for a minimum of 33 runs over each 100 meter segment.

Note: No missed detections in 33 trials indicate a probability of detection greater than 0.91 with a confidence of 95 percent.

Point of Contact:

5.4.7.2

EQUIPMENT EFFECTIVENESS TEST PROCEDURES

Security Measure	Type of Test	Performance Indicator
Ported Coax Cable Sensor (PCCS) (Con't)	Technical Performance	Activate Alarm

Test Method: Roll Test

1. Very slowly roll across the sensor area with the body parallel to the sensor. Arms must be held close to the body and feet together.

. This shall be repeated at intervals of approximately three meters or less

. At least one roll test shall be included over every hardtop surface crossing the sensor.

Note: If failures occur on the hardtop surface, additional tests shall be conducted to determine performance of these locations.

Test Method: Vehicle Test

1. The vehicle test shall be conducted in a straight line in two directions on both sides of the road. Test speeds shall be 8 and 16 km/hr.

Note: Every test should produce an alarm condition.

Note: No missed detections indicate a detection probability greater than 0.97 with a confidence of 95 percent. Five detection failures indicate a probability of detection greater than 0.90 with a confidence level of 95 percent desired. Missed detections should be distributed throughout the sensor zone. Concentrated misses indicate the presence of penetration zones.

Point of Contact:

5.4.7.3

EQUIPMENT EFFECTIVENESS TEST PROCEDURES

Security Measure	Type of Test	Performance Indicator
Individual Resource Protection Sensor (IRPS)	Technical Performance	Activate Alarm

Test Method(s): Walk, Run, Roll, and Vehicle Tests

1. Walk, run, roll, and vehicle tests shall be conducted in the exact same manner for IRPS as for the PCCS.

Note: Performance tests shall be conducted while monitoring the annunciator panel for the presence of an alarm condition. Initial tests shall be made under both normal and water saturated conditions.

Point of Contact:

5.4.7.4

EQUIPMENT EFFECTIVENESS TEST PROCEDURES

Security Measure	Type of Test	Performance Indicator
MILES Buried Cable Sensors	Technical Performance	Activate Alarm

Test Method(s): Walk, Run, Roll, and Vehicle Tests

1. Walk, run, roll, and vehicle tests shall be conducted in the exact same manner for MILES as for the PCCS, (exception, see note 3).

2. The human test subject shall not exceed 68 kg in weight and shall be clear of ferrous material including nails in shoes.

Note 1: Performance tests shall be conducted while monitoring the output relay of the MAID processor for the presence of an alarm condition.

Note 2: Since settling of the soil often results in higher than normal nuisance (false alarm) rates, final tests shall be delayed until about four weeks after installation.

Note 3: Saturated soil tests are not required and testers shall step over the cable marker when conducting the walk and run tests.

Point of Contact:

5.4.7.5

EQUIPMENT EFFECTIVENESS TEST PROCEDURES

Security Measure	Type of Test	Performance Indicator
Bistatic Microwave Sensor (BMS)	Technical Performance	Activate Alarm

Test Method: Walk Test

Before beginning the actual performance tests, a walk test shall be made to assure that movement immediately behind the transmitter and receiver will not activate an alarm. If an alarm is produced, the condition causing the alarm shall be identified and corrected prior to further testing. Failure to correct the condition will likely result in high false alarm rates.

1. If the sensor is located parallel to a fence, a walk test shall be performed to assure proper spacing from the fence.

2. If the unit alarms, significant energy is being reflected off the fence, indicating that the sensor has probably been mounted too close to the fence or misaligned.

   - This may result in high nuisance (false alarm) rates due to wind induced motion of the fence.

Note: Performance tests of each detection zone shall be conducted while monitoring the output relay for the presence of an alarm condition.

Point of Contact:

5.4.7.5

EQUIPMENT EFFECTIVENESS TEST PROCEDURES

Security Measure	Type of Test	Performance Indicator
Bistatic Microwave Sensor (BMS) (Con't)	Technical Performance	Activate Alarm

Test Method: Run Test

1. The run test shall be conducted approximately six meters from the transmitter and from the receiver, where the microwave beam is narrow.

2. The test shall be performed at speeds of approximately 8 m/s.

Test Method: Shuffle-Walk Test

1. The shuffle-walk test is conducted by very slowly walking across the beam without swinging the arms.

   . Step size shall be less than 5 cm.

Test Method: Crawl Test

Ideally, the sensitivity of a microwave system should be adjusted to be the lowest possible gain that will adequately detect the crawling intruder. This technique assures that the nuisance alarm rate is reduced to the lowest possible level.

1. The hardest-to-detect individual maintains the front surface of the body in contact with the ground while moving across the microwave beam.

2. The movement is directly across, keeping the length of the body parallel to the beam in such a manner as to present only the head and shoulders to the receiver or transmitter.

Point of Contact:

5.4.7.5

EQUIPMENT EFFECTIVENESS TEST PROCEDURES

Security Measure	Type of Test	Performance Indicator
Bistatic Microwave Sensor (BMS) (Con't)	Technical Performance	Activate Alarm

Test Method: Crawl/Drag Test

To eliminate actual human crawl tests and to obtain more repeatable results, the crawl test shall be conducted by utilizing an aluminum sphere of 30 cm in diameter.

1. The sphere shall be dragged across the detection zone perpendicular to the microwave beam.

   - The sphere is mounted to a thin non-metallic platform, such as cardboard, and pulled across the zone with a small non-metallic rope. The rope shall be long enough to allow the person pulling the rope to remain outside the microwave beam.

2. Drag tests shall be conducted at one meter intervals over the full detection zone at a speed of 10 cm/s.

   - Tests are not required in offset areas.

Note: Extensive testing has confirmed that this sphere produced detection results very similar to those of a human target.

Note: For a 100 meter segment and 100 crawl/drag test with no misses, the detection probably is estimated to be greater than 0.97 with 95 percent confidence.

Note: If there are five misses, the detection probability is estimated to be 0.90 with a 95 percent confidence level. These misses should be distributed throughout the sensor zone. Concentrated misses indicate the presence of penetration zones.

Point of Contact:

5.4.7.6

EQUIPMENT EFFECTIVENESS TEST PROCEDURES

Security Measure	Type of Test	Performance Indicator
Taut Wire Fence Sensor (TWFS)	Technical Performance	Activate Alarm

Test Method: Simulated Climb

Prior to conducting the test, ensure that:

- The test subject shall not exceed 65 kg in weight
- The covers on each of the sensor switch channels shall be removed (and replaced after testing) to check the operation of the sensor switches
  - Since these switches can be damaged by uncontrolled wire deflecting test shall be terminated immediately when contact closure is affected. (Excessive wire deflection can pull the contact probe out of the contact cup.)

1. The trip wire is tested by leaning a ladder against the tripwire. The tester then climbs the ladder to the point where his knees are as high as the top barbed wire.
   - Contact closure should come at this point or earlier.

Note: Simulated fence climbing tests shall be performed by deflecting the horizontal wires (each wire shall be deflected from both sides of each sensor switch post) since actual climbing or cutting of the wires would very likely damage the switches. This probably would not provide any useful information.

Point of Contact:

5.4.7.6

EQUIPMENT EFFECTIVENESS TEST PROCEDURES

Security Measure	Type of Test	Performance Indicator
Taut Wire Fence Sensor (TWFS) (Con't)	Technical Performance	Activate Alarm

Test Method: Simulated Climb - (Con't)

Note: If installed and properly maintained taut wire fence can be expected to yield a probability of detection of virtually 100 percent for an intruder who climbs or cuts sensor fence, using conventional tools.

Note: Performance tests shall be conducted while monitoring the output relay or the switch line for the presence of an alarm condition.

Point of Contact:

5.4.7.7

EQUIPMENT EFFECTIVENESS TEST PROCEDURES

Security Measure	Type of Test	Performance Indicator
Closed Circuit Television (CCTV)	Technical Performance	Meets Site Requirements

Test Method: Performance Assessment, Review and Evaluation

1. Following system installation, a video recording of all typical day and night camera fields-of-view shall be made

   . The recording should represent the maximum overall performance level attainable with the system, considering video bandwidth, tape format and relative scene illumination.

2. Once a month the recording shall be compared with real-time camera video monitor

   . Observed differences should identify possible system degradation such as change in camera position, poor focus, image deterioration and dynamic range losses.

Note: Since the end product of the CCTV assessment system is one of subjective quality, that is, human interpretation of video images or a monitor screen, a relatively stable reference is required to which current system performance can be compared.

Point of Contact:

5.4.7.8

EQUIPMENT EFFECTIVENESS TEST PROCEDURES

Security Measure	Type of Test	Performance Indicator
Lighting	Technical Performance	Meets Lux Requirements

Test Method: Lux Measurement and Placement Evaluation

1. Perimeter clear zone lighting intensity shall be a minimum of four lux measured on a horizontal plane at ground level

   . A light/dark ratio, that is, brightest point/darkest point, of less than 5 to 1, in the perimeter clear zone is required.

Note: Entry point lighting shall not be considered when evaluating the light/dark ratio for perimeter lighting.

Note: To maximize assessment capability, "hot spots" (very bright areas) shall be avoided.

Note: When power to the lighting system is interrupted, switchover to emergency power should be immediate and the lights should produce full lumin (lux) output within five seconds after being re-energized.

Point of Contact:

5.4.7.9

EQUIPMENT EFFECTIVENESS TEST PROCEDURES

Security Measure	Type of Test	Performance Indicator
Balanced Magnetic Switch Door Sensor	Technical Performance	Activate Alarm

Test Method: Performance Test

1. The test shall be conducted in accordance with installation manuals.

Note: The sensors should not alarm when the door is "rattled" in-and-out.

Point of Contact:

5.4.7.10

EQUIPMENT EFFECTIVENESS TEST PROCEDURES

Security Measure	Type of Test	Performance Indicator
Microphone Sensor	Technical Performance	Activate Alarm

Test Method: Walk Test

Prior to conducting the test, a chalk grid of "walk test" lines shall be made to ensure that the area is completely covered. It is essential that the test team ensure that:

. The target person shall have a height of 1.5 $\pm$ 0.3 meters, and a eight of 59 $\pm$ 5 kg.

1. The target person shall walk with arms folded over his chest.

2. The walk rate shall be at approximately 12 cm/s.

3. Doors will be opened and closed, including locked doors.

4. The entire perimeter and every grid line in the test area shall be walked.

Note: The test shall be repeated three times to identify any "dead spots" in the area covered by the sensor.

Note: The test team should conduct this test with the target person wearing shoes with soft soles made of rubber, or soft cushion material. The test should be conducted also with the person walking barefooted. The test should be conducted with the target person wearing different articles of clothing of different kinds of materials, such as a nylon jacket, a cotton shirt, a wool jacket. This test will provide an indication of the sensitivity of the microphone sensors to variations in target's apparel.

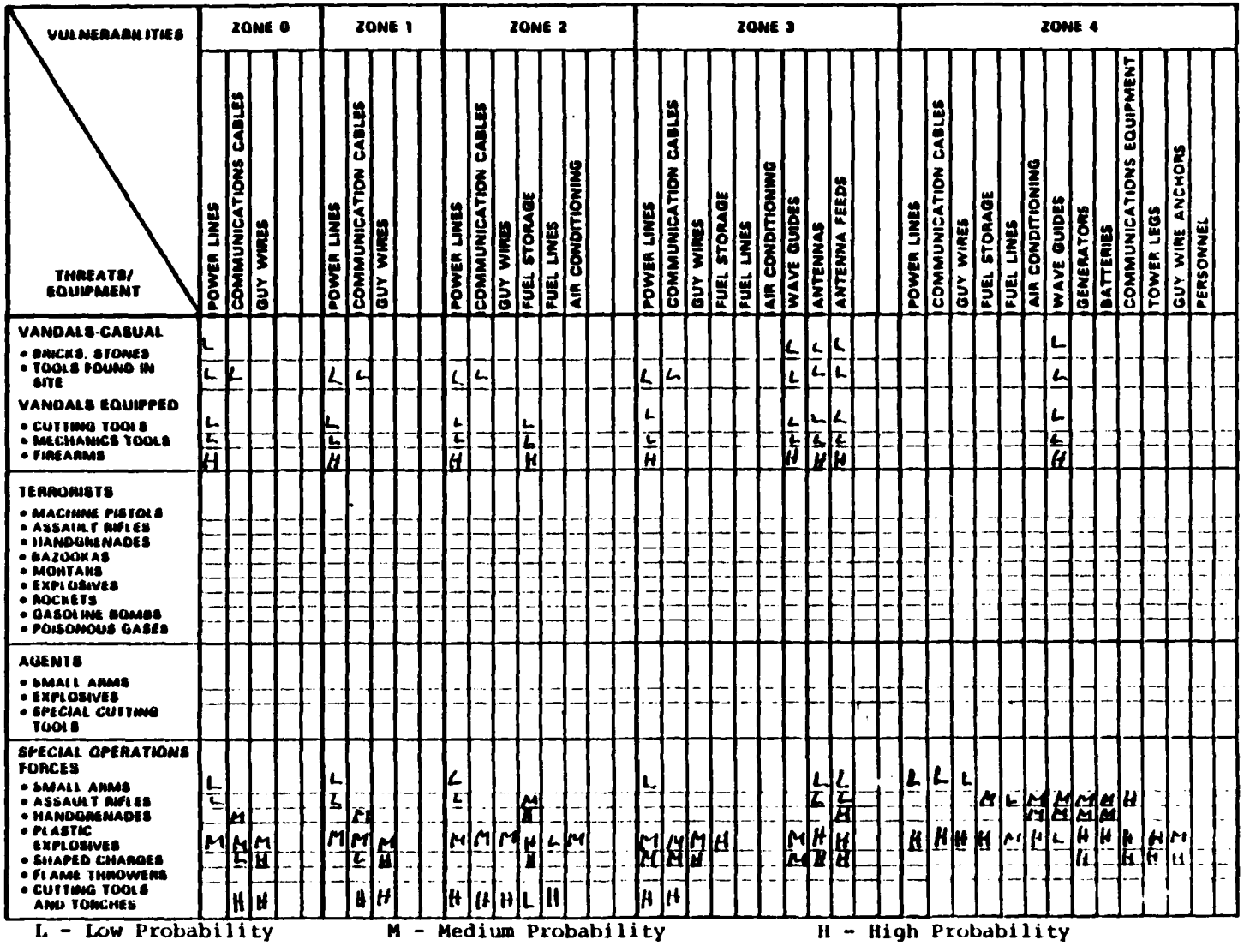
Point of Contact:

THREAT TYPE	POSSIBLE THREAT MOTIVATION(s)	ESTIMATED SIZE RANGES	CAPABILITIES/TRAINING	DCS TARGET TYPE: CRITICALITY/LOCATION
VANDALS (pilferage, theft, break-ins, pranks)	Desire for personal material gain; excitement/amusement/ entertainment. Possibly mental instability or political malcontentment.	A single participant; may be several persons. (Possibly a group in the context of political demonstrations.)	- No special training. - Hunting arms; heavy, throwable objects (stones, bricks, etc.); assorted small (pocket) objects— knives, wire cutters, etc.	Unmanned or lightly manned; remote or in vicinity of homesteaders or the public.
TERRORISTS	To publicize a cause by means of publicity; desire psychological effect. Anti-American/ "imperialist" sentiments.	Range of between 2-10 terrorists	- Well-trained, specialization among group members. Guerrilla warfare. - Equipment/Armament: Usually small and concealable. May include machine pistols, assault rifles, submachine guns, explosives, hand grenades, smoke bombs, bazookas, mortars. Possibly rockets, mustard gas/nerve agents.	Probably manned, high visibility facility that is very obviously a military (and possibly an American) installation.
FOREIGN AGENTS	To threaten the operations, facilities, or personnel of the DCS with damage and/or destruction for the purpose of disrupting DCS operations and/or embarrassing and harrassing the U.S. and/or host country.	A single agent; possibly a small team	- Well-trained experts. - Equipment/Armament: small arms (see listing under terrorism), explosives, detonating devices, communications equipment to interface with other operatives and/or "command" center.	Critical DCS nodes, unmanned and manned.
SPECIAL OPERATIONS FORCES (SOFs)	Disrupt or destroy DCS operations from peacetime through war by means of unconventional military operations.	Range of between 7-17 men	- Highly skilled in sabotage/ unconventional warfare. - Equipment/Armament: Receive best available weapons to perform mission, may include: anti-tank guns, snipers' rifles, assault rifles, grenades and launchers, rocket launchers.	Critical DCS nodes, unmanned and manned.

TABLE 1. A Summary of Threat Categories and Motives

VULNERABILITIES / THREATS/EQUIPMENT	ZONE 0			ZONE 1			ZONE 2						ZONE 3								ZONE 4										
	POWER LINES	COMMUNICATIONS CABLES	GUY WIRES	POWER LINES	COMMUNICATION CABLES	GUY WIRES	POWER LINES	COMMUNICATION CABLES	GUY WIRES	FUEL STORAGE	FUEL LINES	AIR CONDITIONING	POWER LINES	COMMUNICATION CABLES	GUY WIRES	FUEL STORAGE	FUEL LINES	AIR CONDITIONING	WAVE GUIDES	ANTENNAS	ANTENNA FEEDS	POWER LINES	COMMUNICATION CABLES	GUY WIRES	FUEL STORAGE	FUEL LINES	AIR CONDITIONING	WAVE GUIDES	GENERATORS	BATTERIES	COMMUNICATIONS EQUIPMENT	TOWER LEGS	GUY WIRE ANCHORS	PERSONNEL
VANDALS-CASUAL • BRICKS, STONES • TOOLS FOUND IN SITE																																	
VANDALS-EQUIPPED • CUTTING TOOLS • MECHANICS TOOLS • FIREARMS																																	
TERRORISTS • MACHINE PISTOLS • ASSAULT RIFLES • HANDGRENADES • BAZOOKAS • MORTARS • EXPLOSIVES • ROCKETS • GASOLINE BOMBS • POISONOUS GASES																																	
AGENTS • SMALL ARMS • EXPLOSIVES • SPECIAL CUTTING TOOLS																																	
SPECIAL OPERATIONS FORCES • SMALL ARMS • ASSAULT RIFLES • HANDGRENADES • PLASTIC EXPLOSIVES • SHAPED CHARGES • FLAME THROWERS • CUTTING TOOLS AND TORCHES																																	

Table 2. Threat-Vulnerability Matrix



L - Low Probability M - Medium Probability H - High Probability

Table 2a. Threat-Vulnerability Matrix with Sample Threat Estimate

Table 3 L.O.S. Repeater Threat Profile

Threat Type	Capabilities
Vandals	- Single or several persons - No special training - Hunting arms - No penetration tools
Terrorists	- None
Agents	- None
Special Operations Forces	- 3-12 combatants - Highly skilled in sabotage/ unconventional warfare - Armed and carrying explosives

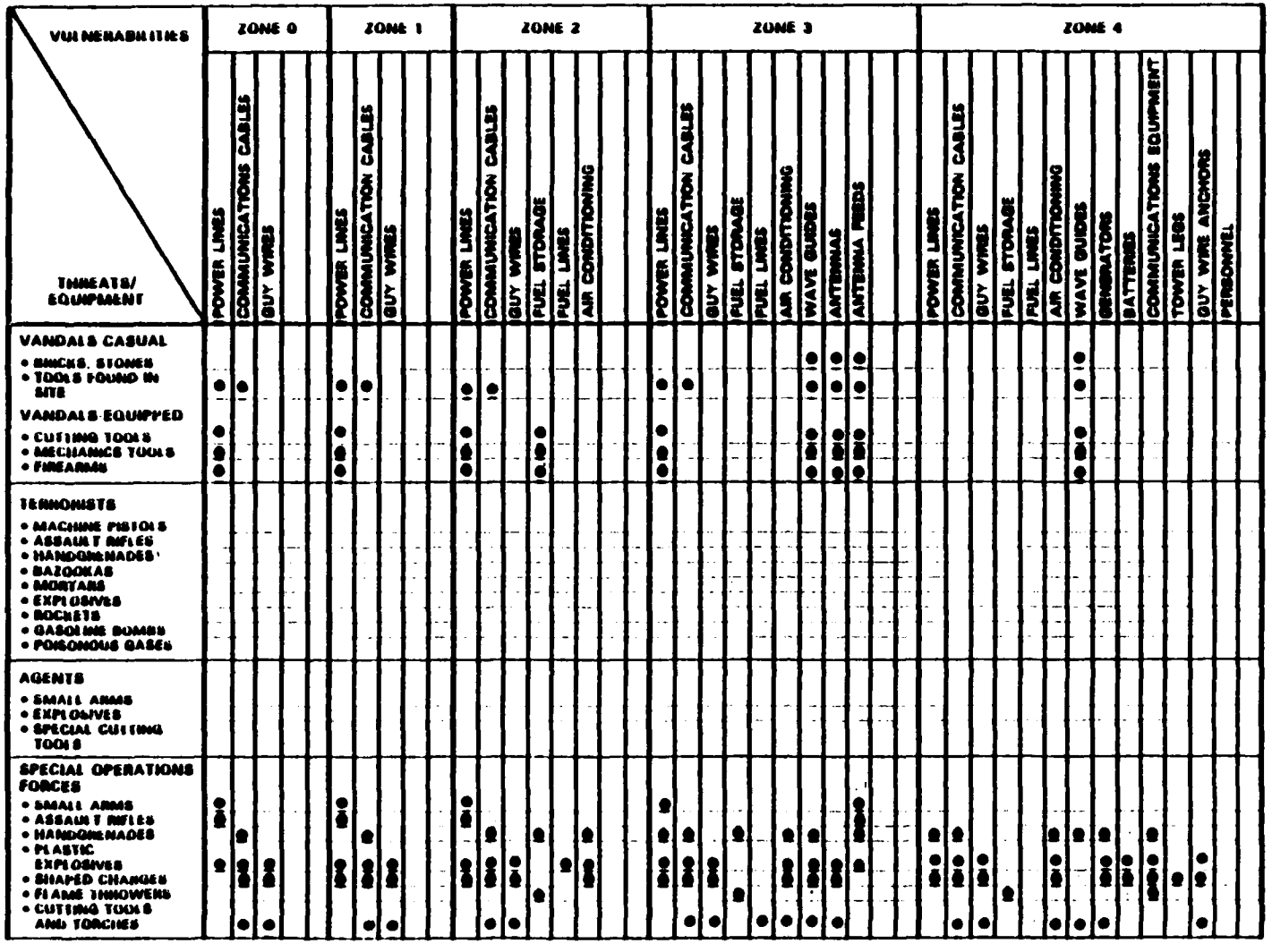


Table 4. Threat Vulnerability Matrix - Site: L.O.S. Repeater (Unmanned)

Table 5 Satellite Station Threat Profile

Threat Type	Capabilities
Vandals	- None
Terrorists	- 2 to 8 persons - Well trained - Armed but small quantities of explosives
Agents	- 6 to 8 persons - Well trained - Armed and carrying explosives
Special Operations Forces	- None

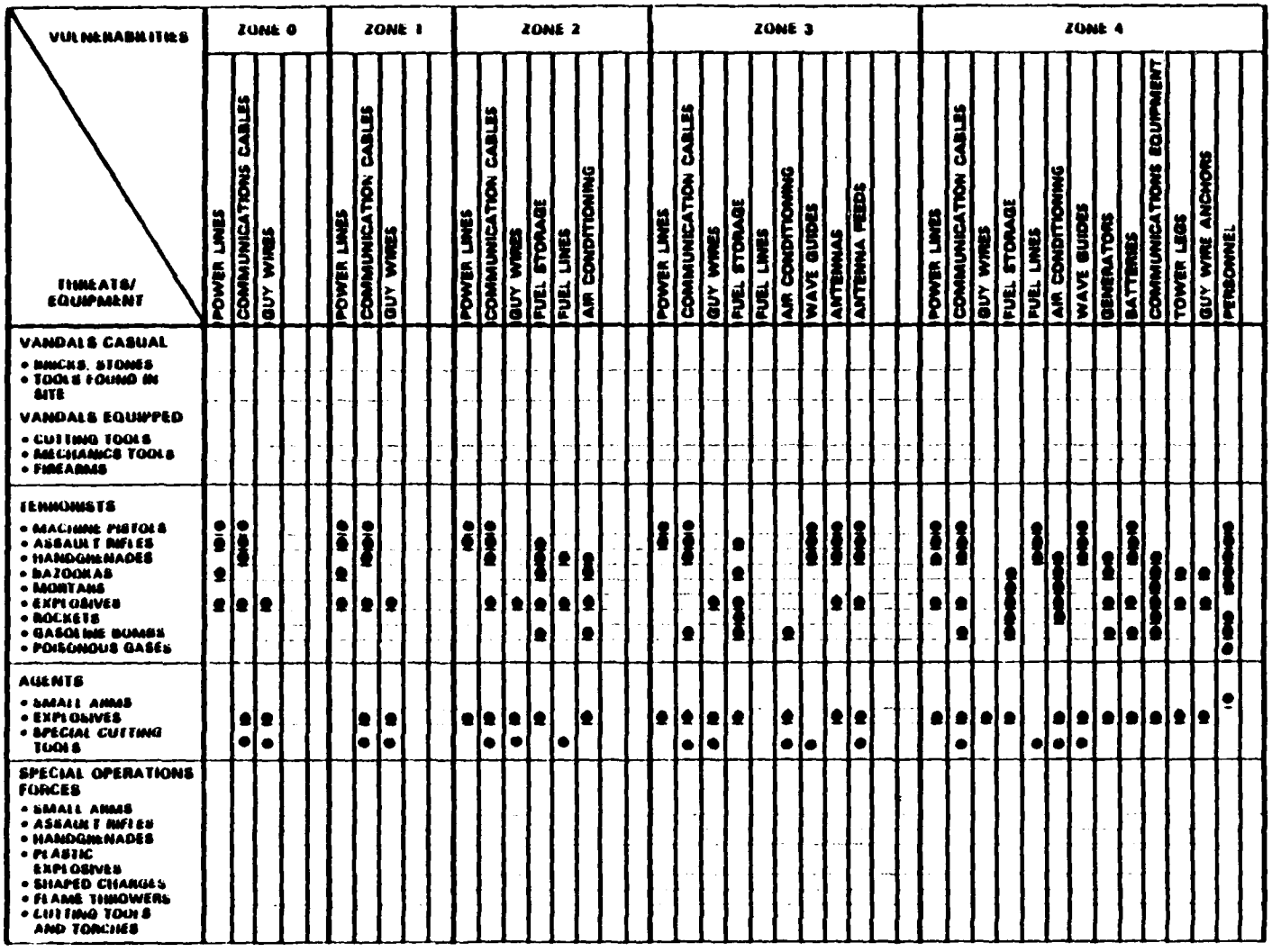


Table 6. Threat Vulnerability Matrix - Site:
Satellite Ground Terminal

TABLE 7
Site Characteristics to be Evaluated to Determine Appropriate Sensor Selection

Site Variations	- Soil conditions, pavement, ground freeze, streams, terrain, water lines, sewers, fence pole locations, buildings, underground cables
Environment	- Temperature, wind, rain, snow, wild life, thunder, lightning, earth vibrations, vegetation
Inherent Component Characteristics	- Sensor-to-sensor interactions, upkeep cost, stability, capability limitations, self-test, false alarm rate, probability of detection, cost, reliability, repeatability, tamper resistance
Man-Made Disturbances	- Underground telephone and power cables, generators, motors, power transformers, radio, TV, radar, communications equipment, vehicle ignition, auto, train or aircraft vibrations
Human Engineering	- Ease of installation, ease of maintenance, assessment, reporting, personnel requirements
Interfaces	- Hardware/hardware, hardware/human, sensor/junction, sensor/data transmission links, sensor/power source available, sensor/installation hardware, sensor/tamper protection
Documentation	- Procurement, acceptance, installation, maintenance, software requirements, operational procedures, periodic checks, orderly checkout, test plans
Adversary Attributes	- Threat level, tools, weapons, methods or entry

TABLE 8. LIST OF SENSORS APPLICABLE TO ZONE ONE

	SENSOR/SENSOR TYPE	SOURCE
1.	Ported Coaxial Cable (PCC)	Military
2.	Individual Resource Protection Sensor (IRPS)	Military
3.	Magnetic Intrusion Line Sensor (MILES)	Military
4.	Bistatic Microwave	Commercial
5.	Point Sensor (Electromagnetic)	Military
6.	Electric Field Fence (EFF)	Commercial
7.	Laser Fence Sensor	Military
8.	Infrared Fence Sensor (IRCCD)	Military

VULNERABILITIES	ZONE 0					ZONE 1					ZONE 2										ZONE 3										ZONE 4													
	POWER LINES	COMMUNICATION CABLES	GUY WIRES			POWER LINES	COMMUNICATION CABLES	GUY WIRES			POWER LINES	COMMUNICATION CABLES	GUY WIRES	FUEL STORAGE	FUEL LINES						POWER LINES	COMMUNICATION CABLES	GUY WIRES	FUEL STORAGE	FUEL LINES	AIR CONDITIONING	WAVE GUIDES	ANTENNAS	ANTENNA FEEDS	AIR CONDITIONING		POWER LINES	COMMUNICATIONS CABLES	GUY WIRES	FUEL STORAGE	FUEL LINES	AIR CONDITIONING	WAVEGUIDES	GENERATORS	BATTERIES	COMMUNICATIONS EQUIPMENT	TOWER LEGS	GUY WIRE ANCHORS		
PROTECTION MEASURES	b	b				a c d g	a c d g	a c r			a c g i	a c g i	a c r	a c f g	a c i g						a c g h k m n o	a c g h k m n o	a c r	a c g h k m n o	a c g h k m n o	a c g h j	a c g q	a c g p	a c g p	a c g h		a c g h k m n o s	a c g h k m n o s	a c g u	a c g h k m n o s	a c g h k m n o s	a c g h j k m n o q s	a c g h j m n o q s	a c g h k m n o s	a c g h k m n o s	a c g h k m n o s	a c g k l n s	a c g u		

Table 9. Vulnerabilities - Security Measures Matrix

KEY	APPLICABLE PARAGRAPHS (SECURITY MEASURES)
a	5.1.3.2.1 - 5.1.3.2.1.4 (Access Road), 5.1.3.2.2 (Sensors), 5.1.3.2.3 (Alarm Assessment), 5.1.3.2.4 (Cleared Area), 5.1.3.3.1 - 5.1.3.3.1.6 (Perimeter Fence), 5.1.3.3.3 (Warning Signs), 5.1.3.3.4 (Cleared Area), 5.1.3.3.5 (Locks and Keys), 5.1.3.3.6 (Sensors), 5.1.3.3.7 (Alarm Assessment), 5.1.3.4.1 - 5.1.3.4.1.5 (Inner Fence), 5.1.3.4.2 (Sensors), 5.1.3.4.3 (Alarm Assessment)
b	5.1.3.2.5 (Cables)
c	5.1.3.3.2 - 5.1.3.3.2.2 (Site Entry Control), 5.1.3.4.9 - 5.1.3.4.9.5 (Guard Force Procedures), 5.1.3.5.4 (Entry Control)
d	5.1.3.3.8 (Cables)
e	5.1.3.4.4 (Non-Critical Buildings)
f	5.1.3.4.5 (Fuel Storage)
g	5.1.3.4.6 (Lighting)
h	5.1.3.4.7 (Gabion)
i	5.1.3.4.9 (Cables)
j	5.1.3.4.10 (Air Conditioning)
k	5.1.3.5.1 (Critical Buildings)

Table 10. Vulnerabilities - Security Measures Matrix Key

KEY	APPLICABLE PARAGRAPHS (SECURITY MEASURES)
l	5.1.3.5.2 (Tower Barriers)
m	5.1.3.5.3 (Obscurants)
n	5.1.3.5.5 (Doors, Windows, and Other Openings)
o	5.1.3.5.6 (Sensors), 5.1.3.5.7 (Alarm Assessment)
p	5.1.3.5.8 (Radomes)
q	5.1.3.5.9 (Waveguide Protection)
r	5.1.3.5.10 (Guy Wire Protection)
s	5.1.3.5.6.1 (Protection of Critical Equipment)
t	5.1.3.5.6.2 (Tower Leg Protection)
u	5.1.3.5.6.3 (Guy Wire Anchors)

Table 10. (Continued)

Site Name (Microwave L.O.S.) Unmanned

Threat Vandal Site Criticality low

	ZONE 0					ZONE 1					ZONE 2										ZONE 3										ZONE 4												
	POWER LINES	COMMUNICATION CABLES				POWER LINES	COMMUNICATION CABLES				POWER LINES	COMMUNICATION CABLES		FUEL STORAGE	FUEL LINES						POWER LINES	COMMUNICATION CABLES		FUEL STORAGE	FUEL LINES	AIR CONDITIONING	WAVE GUIDES	ANTENNAS	ANTENNA FEEDS	AIR CONDITIONING			POWER LINES	COMMUNICATIONS CABLES		FUEL STORAGE	FUEL LINES	AIR CONDITIONING	WAVEGUIDES	GENERATORS	BATTERIES	COMMUNICATIONS EQUIPMENT				
Bury cables	●	●				●	●				●	●																														
Install fence						○	○				○	○		○	○						○	○		○	○	○	○	○	○	○			○	○		○	○	○	○	○	○	○			
Bury Fuel Tanks														●	●																												
Relocate air conditioning																														○														
Install security door																					●	●		●	●	●							●	●		●	●	●	●	●	●	●			
Cover windows																					●	●		●	●	●							●	●		●	●	●	●	●	●	●			
Enclose waveguide																											●																

LEGEND:

● - High Level of Protection

○ - Medium Level of Protection

Blank - No Protection

Table 11. Example Protection Allocation Matrix

Table 12

Sample Unique Site Characteristics and Related Susceptibilities

Unique Site Characteriscties	Associated Susceptibilities
. Site located on hill side; microwave antenna on building roof; roof level with public parking lot.	. Microwave antenna susceptible to hand gun fire; vehicle may be rolled from parking lot and crashed onto roof of building.
. Building exterior wall adjacent to public thorough-fare.	. Equipment located along interior wall subject to blast or wall collapse.
. Facility located as tenant in building.	. Prime and stand-by power shared with other tenants; power outside secure area.
. Large, low frequency antenna system suspended on wooden poles.	. Antenna structure subject to destruction using simple tools, light explosives, venicle ramming.

SECURITY EQUIPMENT	TEST METHOD	DATE TESTED	RESULTS	
			SAT.	UNSAT.
1. Access Road Sensor	1. Vehicle Test			
2. Ported Coaxial Cable Sensor (PCCS)	1. Walk Test			
	2. Run Test			
	3. Roll Test			
	4. Vehicle Test			
3. Individual Resource Protection Sensor (IRPS)	1. Walk Test			
	2. Run Test			
	3. Roll Test			
	4. Vehicle Test			
4. Miles Buried Cable Sensor	1. Walk Test			

TABLE 13. Security Equipment Effectiveness Test Checklist

SECURITY EQUIPMENT EFFECTIVENESS TEST CHECKLIST

SECURITY EQUIPMENT	TEST METHOD	DATE TESTED	RESULTS SAT.	RESULTS UNSAT.
4. Miles Buried Cable Sensor (Cont'd)	2. Run Test			
	3. Roll Test			
	4. Vehicle Test			
5. Bistatic Microwave Sensor	1. Walk Test			
	2. Run Test			
	3. Shuffle-Walk Test			
	4. Crawl Test			
	5. Crawl/Drag Test			
6. Taut Wire Fence Sensor (TWFS)	1. Simulate Fence Climb (Wire Deflection)			
	2. Ladder Climb			

TABLE 13. (Cont'd)

SECURITY EQUIPMENT EFFECTIVENESS TEST CHECKLIST

SECURITY EQUIPMENT	TEST METHOD	DATE TESTED	RESULTS	
			SAT.	UNSAT.
7. Closed Circuit Television (CCTV)	1. Performance Assessment, Review and Evaluation			
8. Lighting	1. Lux Measurement & Placement Evaluation			
9. Balanced Magnetic Switch Door Sensor	1. Performance Evaluation Per Installation Manual			
10. Microphone Sensor	1. Grid-Perimeter Walk Test			

TABLE 13. (Cont'd)

	SITE APPLICATION		EFFECTIVENESS RATING				
			VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
SECURITY EQUIPMENT	EXISTING	NEW	1	2	3	4	5
1. Access Road Sensor							
2. Ported Coaxial Cable Sensor							
3. Individual Resource Protection Sensor							
4. Miles Buried Cable Sensor							

TABLE 14. Security Equipment Effectiveness Rating Checklist

	SITE APPLICATION		EFFECTIVENESS RATING				
			VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
SECURITY EQUIPMENT	EXISTING	NEW	1	2	3	4	5
5. Bistatic Microwave Sensor							
6. Taut Wire Fence Sensor							
7. Closed Circuit Television (CCTV)							
8. Lighting							

TABLE 14. (Cont'd)

	SITE APPLICATION		EFFECTIVENESS RATING				
			VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
SECURITY EQUIPMENT	EXISTING	NEW	1	2	3	4	5
9. Balanced Magnetic Switch Door Sensor							
10. Microphone Sensor							

TABLE 14. (Cont'd)

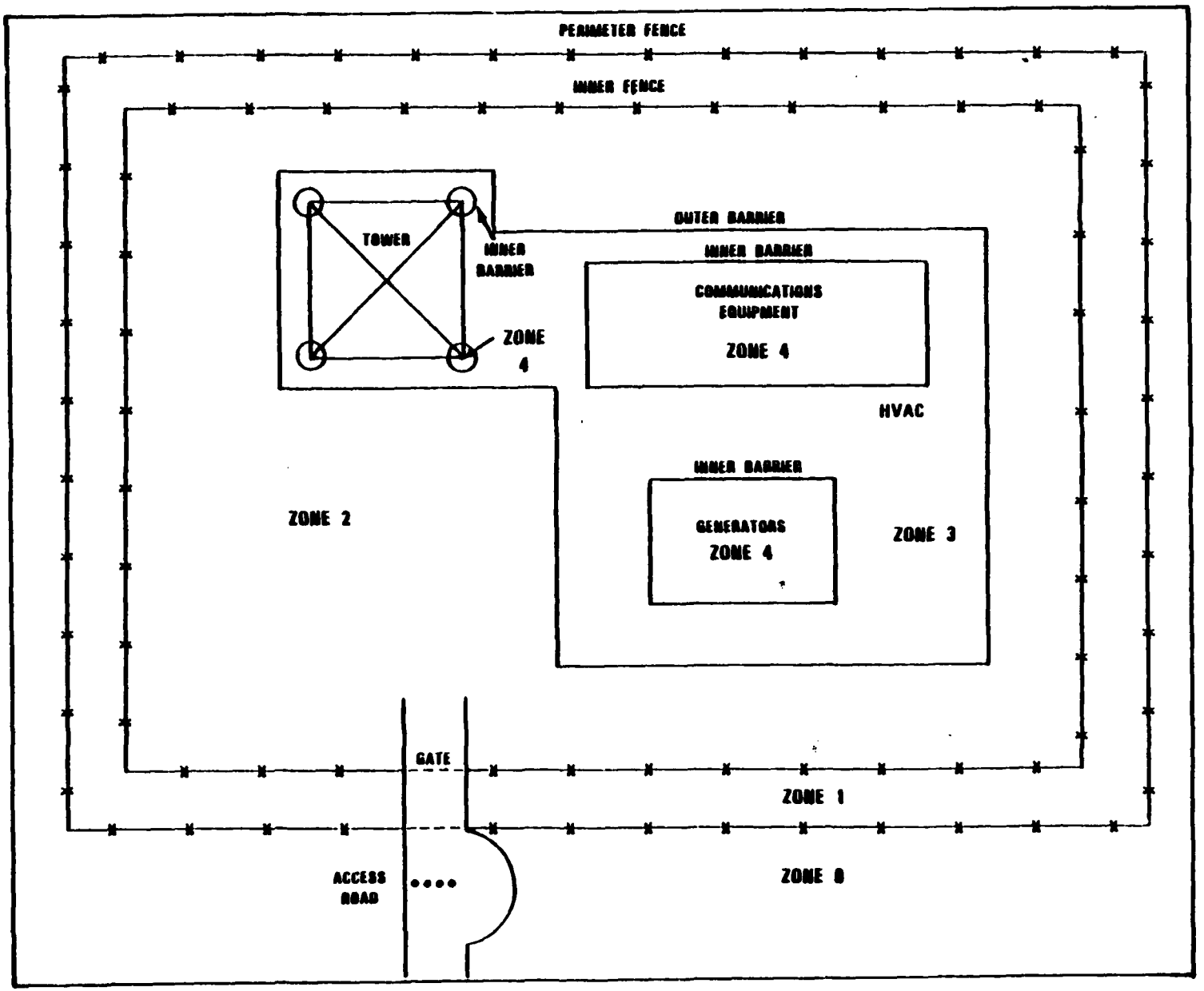


Figure 1. Example of Security Zones for a Generic Unmanned DCS Site.

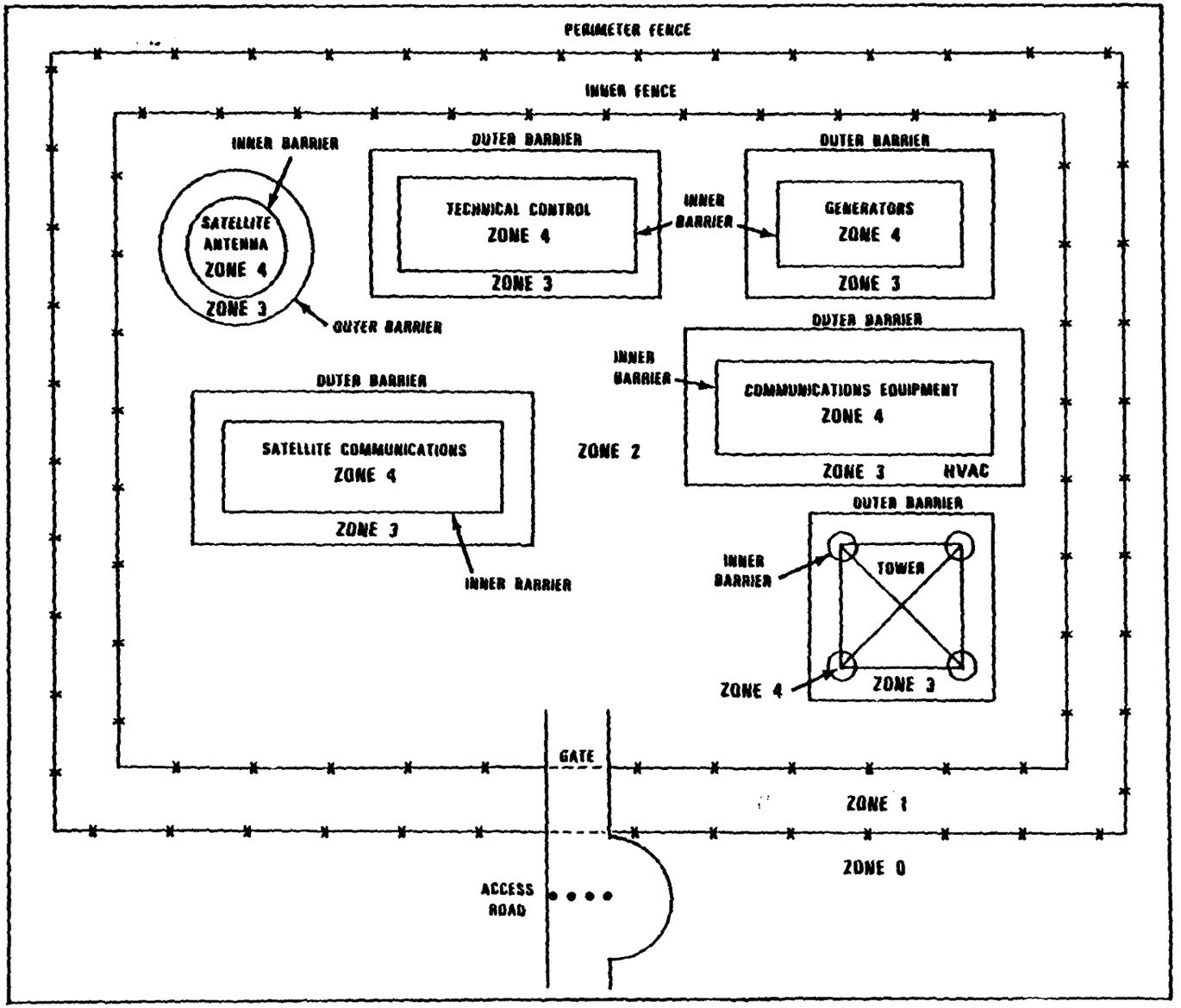


Figure 2. Example of Security Zones for a Generic Manned DCS Site.

VEHICLE BARRIERS

Description - Vehicle barriers shall consist of the use of W-beam guard rail supported on S-beam posts to preclude the use of a vehicle in an unauthorized penetration of the site perimeter.

Installation - Vehicle barriers shall be positioned to prevent straight line approaches by vehicles to the perimeter fence and gate (Figures a and b). The vehicle barrier shall consist of galvanized steel W-beam guard rail in accordance with Figure c.

Maintenance - All joints and hardware shall be painted after assembly to prevent rust. Vehicle barriers shall be inspected every 6 months for damage or wear.

References - Location, Selection and Maintenance of Highway Guardrails and Median Barriers, National Cooperative Highway Research Program Report 54, Southwest Research Institute, San Antonio, Texas, 1968.

Figure 3. Vehicle Barriers

VEHICLE BARRIERS (Continued)

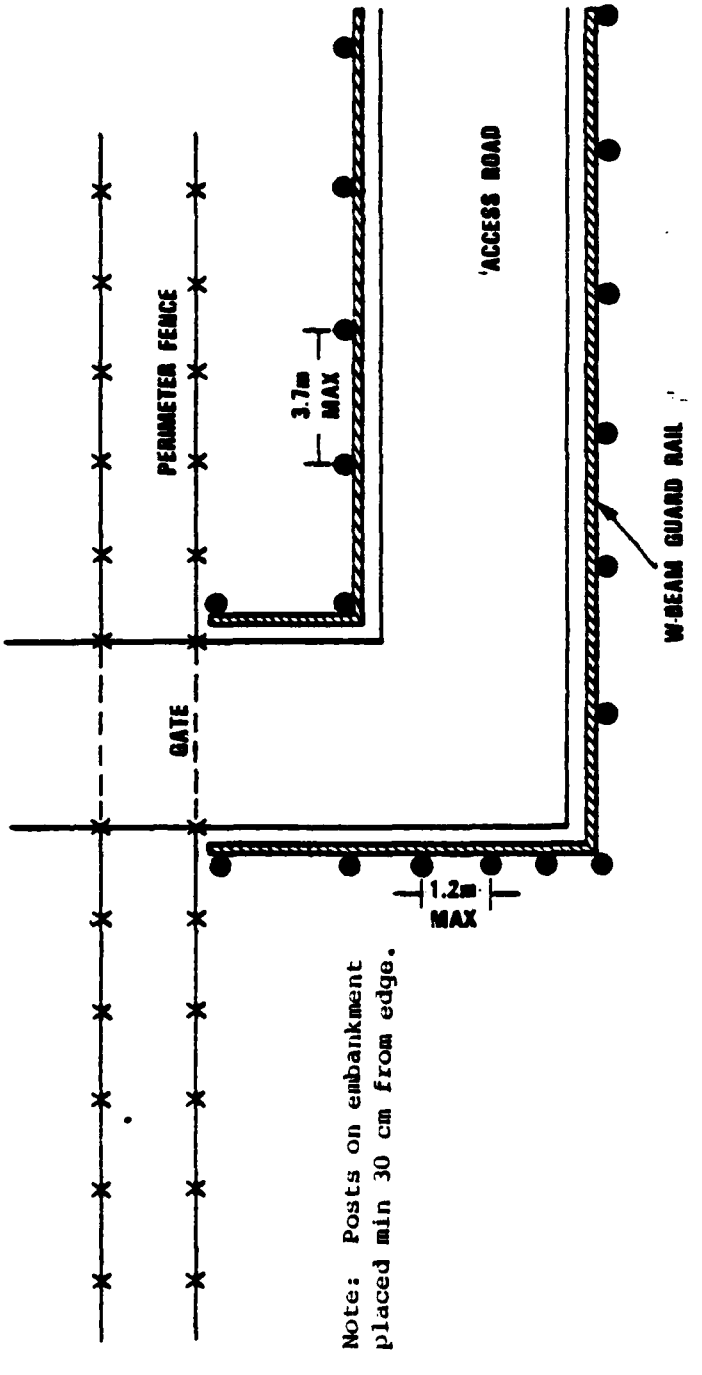


Figure a.

Figure 3. (Continued)

VEHICLE BARRIERS (Continued)

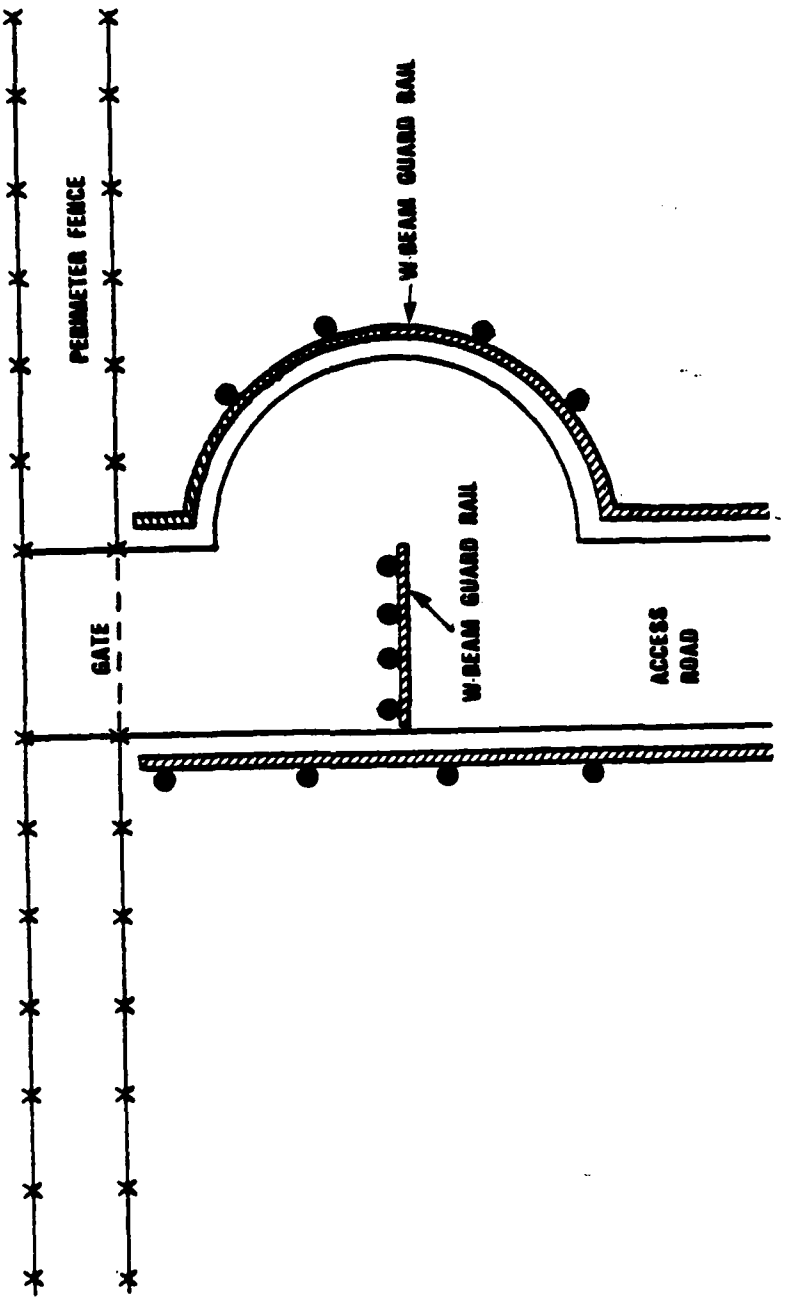


Figure b.

Figure 3. (Continued)

VEHICLE BARRIERS (Continued)

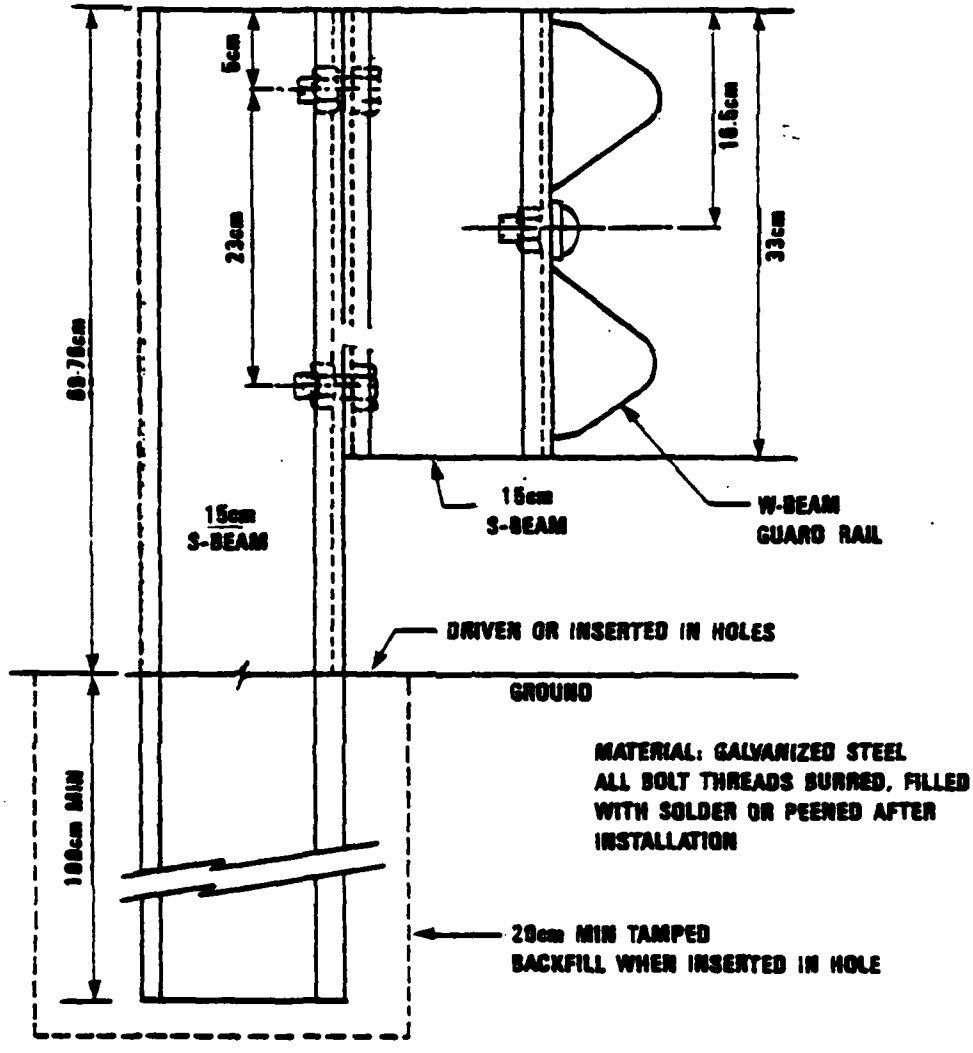


Figure c.

Figure 3. (Continued)

VEHICULAR CONTROL GATE

Description - A vehicular control gate shall consist of the use of a swingable crash beam supported on posts located near the entrance to the site access road to preclude unauthorized traffic along the access road and to prevent a casual vehicle from being sensed by the access road sensor (Figure a). Vehicle-barriers shall be used to prevent a vehicle from circumventing the control gate.

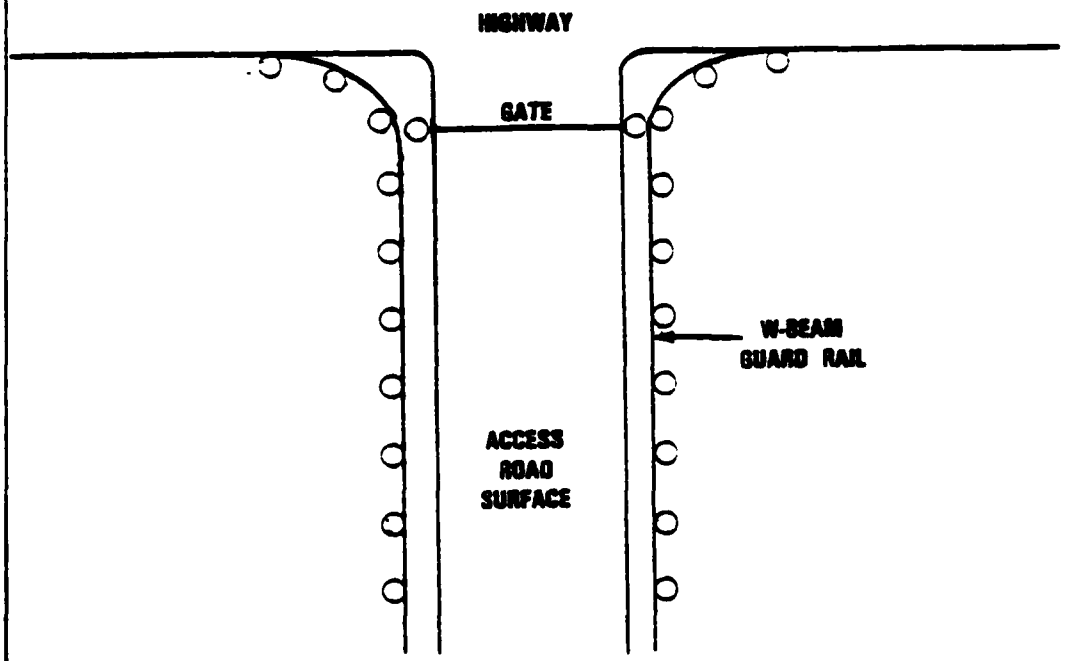


Figure a.

Figure 4. Vehicular Control Gate

VEHICULAR CONTROL GATE (Continued)

Installation - The vehicular control gate shall be constructed in accordance with Figure b. The crash beam may be hinged to open vertically or to swing horizontally.

Maintenance - All joints and hardware shall be painted after assembly to prevent rust. The vehicular control gate shall be inspected every 6 months for damage or wear.

References - Physical Security, U.S. Army Field Manual 19-30, March 1979.

U.S. Army, Office, Chief of Engineers Drawing 40-16-10.

Figure 4. (Continued)

VEHICULAR CONTROL (Continued)

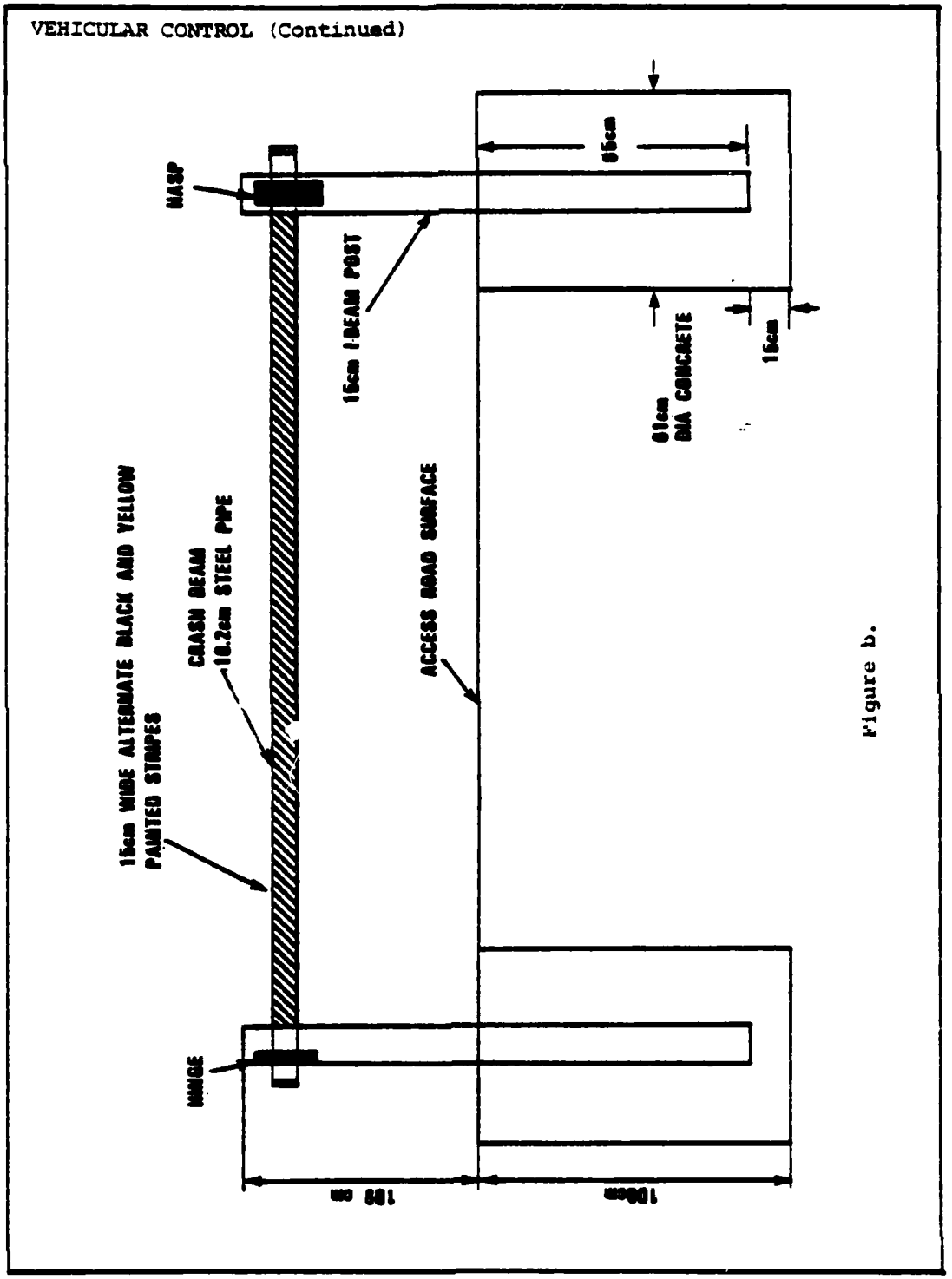


Figure b.

Figure 4. (Continued)

ACCESS ROAD SENSOR

Description - The access road sensor shall consist of an active loop detector buried in the access roadway as indicated in Figure a. When an approaching vehicle traverses the roadway wire loop, the vehicle's metal changes the inductance of the loop, producing an alarm condition.

Installation - The access road sensor wire shall be placed at the bottom of a saw cut (Figure b) and laid in the slot so that there are no kinks or curls, and no straining or stretching of the insulation. All loops shall be wired in the counter-clockwise direction. The wire shall be tamped with a wooden stick in a way that will not cut the wire. Any wire with cuts, breaks, or nicks in the insulation shall be replaced. The wire shall be installed so that each loop is pressed to the bottom of the slot and against one another. Saw cuts shall be made in accordance with Figure c and overlapped so the slot has full depth at all corners. All corners shall be rounded smooth.

Figure 5. Access Road Sensor

ACCESS ROAD SENSOR (Continued)

Maintenance - Periodic performance testing shall be performed. If the sensor is suspected of degraded performance, testing shall be initiated.

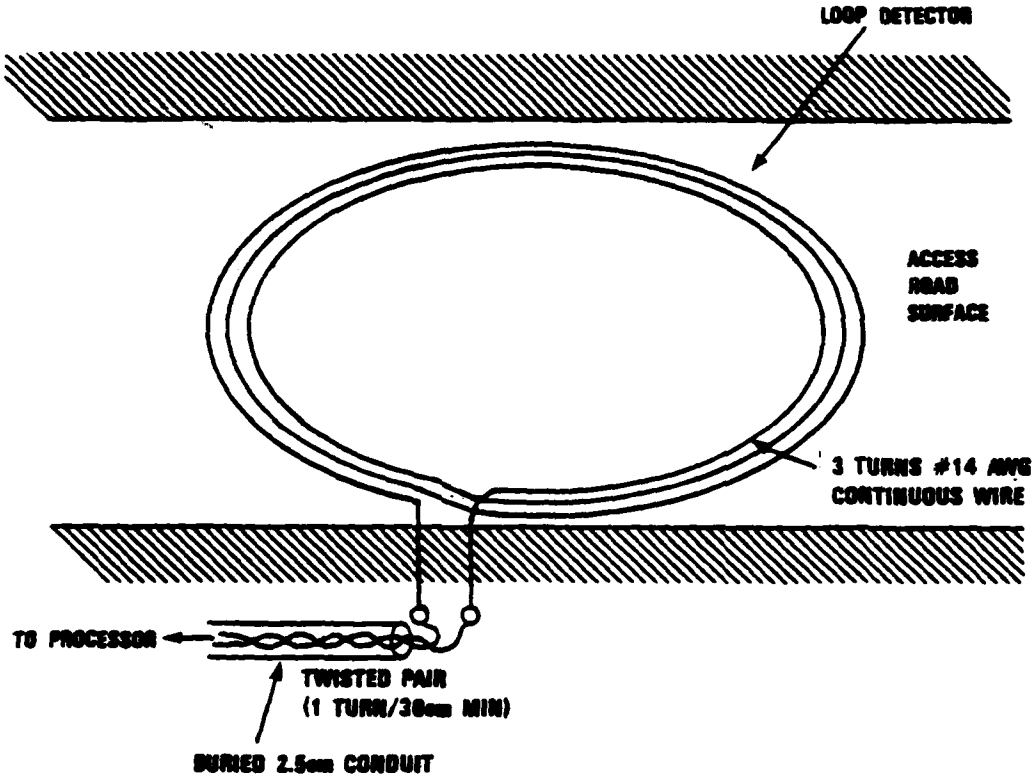


Figure a.

Figure 5. (Continued)

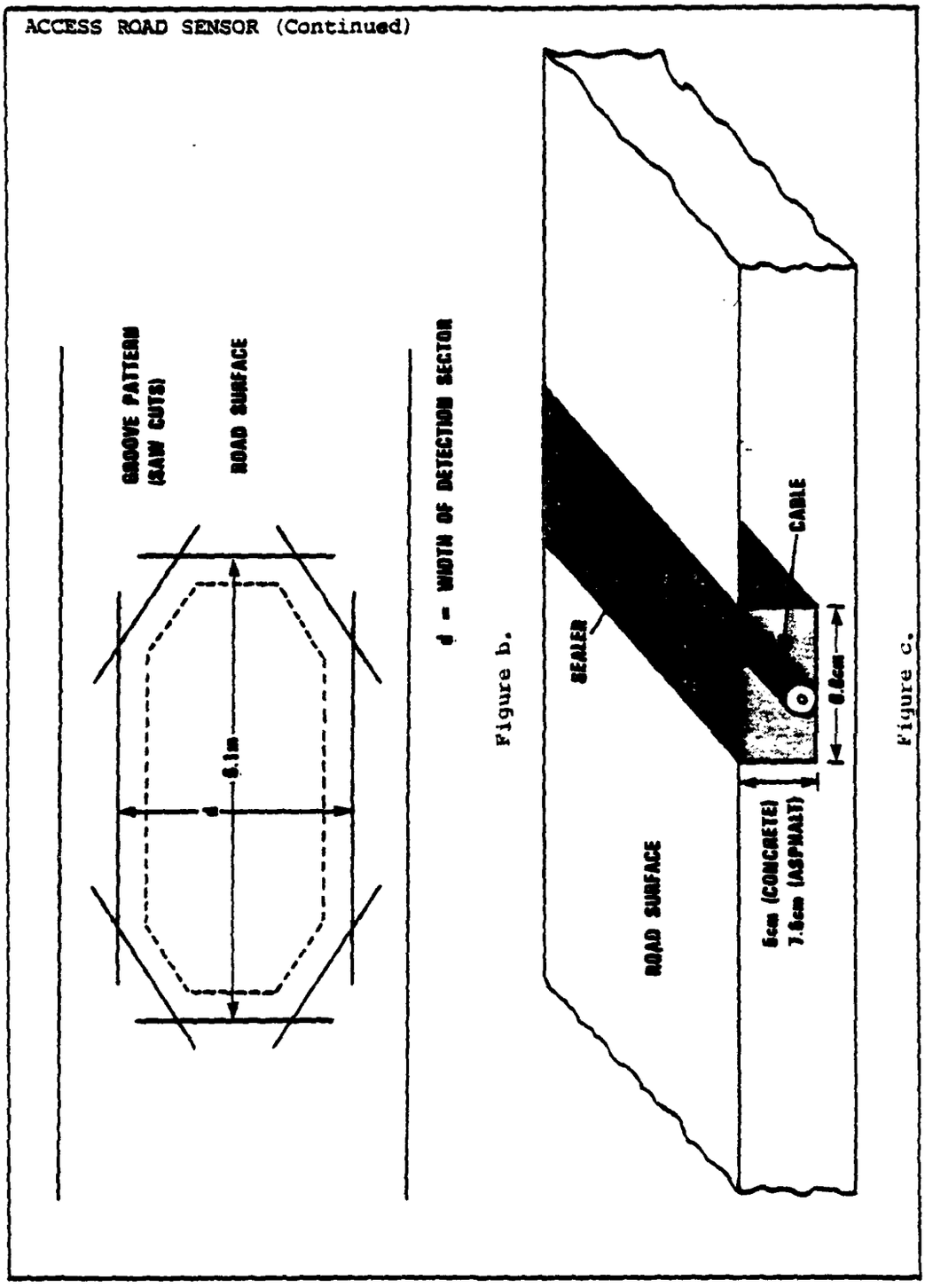


Figure 5. (Continued)

FENCE

Description - A continuous fence shall be employed around all DCS sites to deter casual intruders.

Installation - Fences shall be constructed in accordance with Figure a, with additional bracing at corners and gates. All posts and bracings shall be mounted inside the fence fabric. The fence shall be topped as indicated in Figure b. Where the fence fabric runs over immovable rock, the fabric shall be positioned within 5 cm of ground level and attached to a 4.1 cm steel bottom rail or taut wire to prevent lifting of the fabric.

Figure a.

Figure 6. Fence

FENCE (Continued)

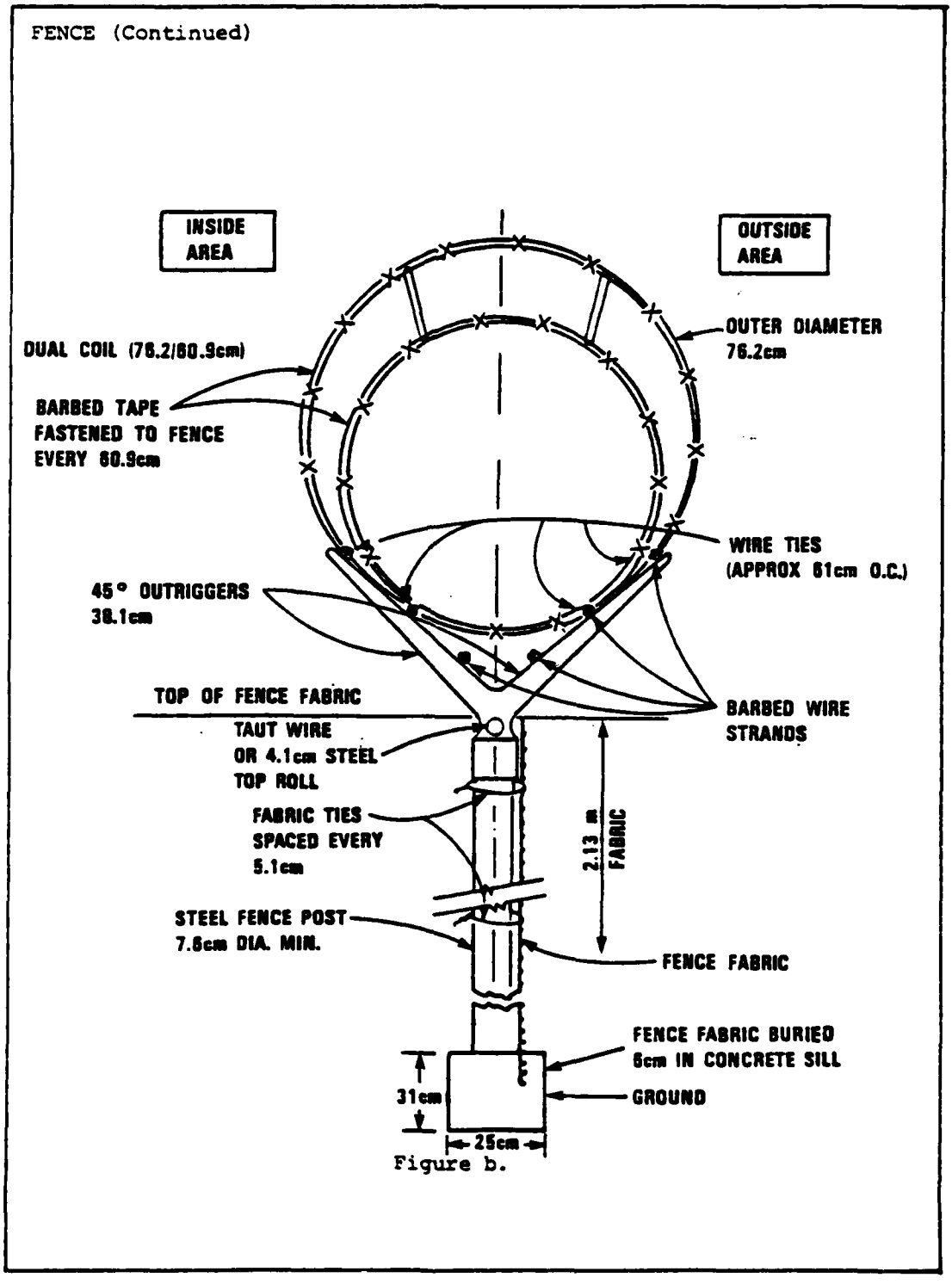


Figure b.

Figure 6. (Continued)

FENCE (Continued)

Maintenance - Fences shall be inspected daily at manned DCS sites and upon every visit to unmanned sites. Fences shall be inspected for damage, wear or tampering, erosion of soil, loosened fittings or growth of vegetation in the clear areas. Necessary repairs or replacements shall be made as soon as possible. Grid barriers in drainage openings or culverts shall be cleared of debris.

References - Physical Security, U.S. Army Field Manual 19-30, March 1979.

U.S. Army, Office, Chief of Engineers, Drawing 40-16-10.

U.S. Federal Specification RR-F-191/1 Type I.

U.S. Military Federal Specification MIL-B-52775A.

Figure 6. (Continued)

FENCE GATE

Description - A DCS site shall employ single or double leaf gates on fences for authorized access of personnel and maintenance vehicles.

Installation - Gates shall be constructed in accordance with Figure a. All posts, bracing and hardware shall be mounted inside the gate fabric. All gate hardware shall be peened and welded to prevent removal. Gates shall be topped in the same manner as the adjacent fencing unless that configuration interferes with the operation of the gate in which case a "Y" outrigger may be set at 45 degrees or replaced by a single vertical arm.

Maintenance - Gates shall be inspected daily at manned sites and upon every visit at unmanned sites. Gates shall be inspected for damage, wear and tampering, and loosened fittings. If a gate has been degraded, effectual repairs shall be made as soon as possible.

References - Physical Security, U.S. Army Field Manual 19-30, March 1979.

U.S. Army, Office, Chief of Engineers Drawing 40-16-10.

U.S. Federal Specification RR-F-191/1 Type I.

U.S. Military Federal Specification MIL-B-52775A.

Figure 7. Fence Gate

FENCE GATE (Continued)

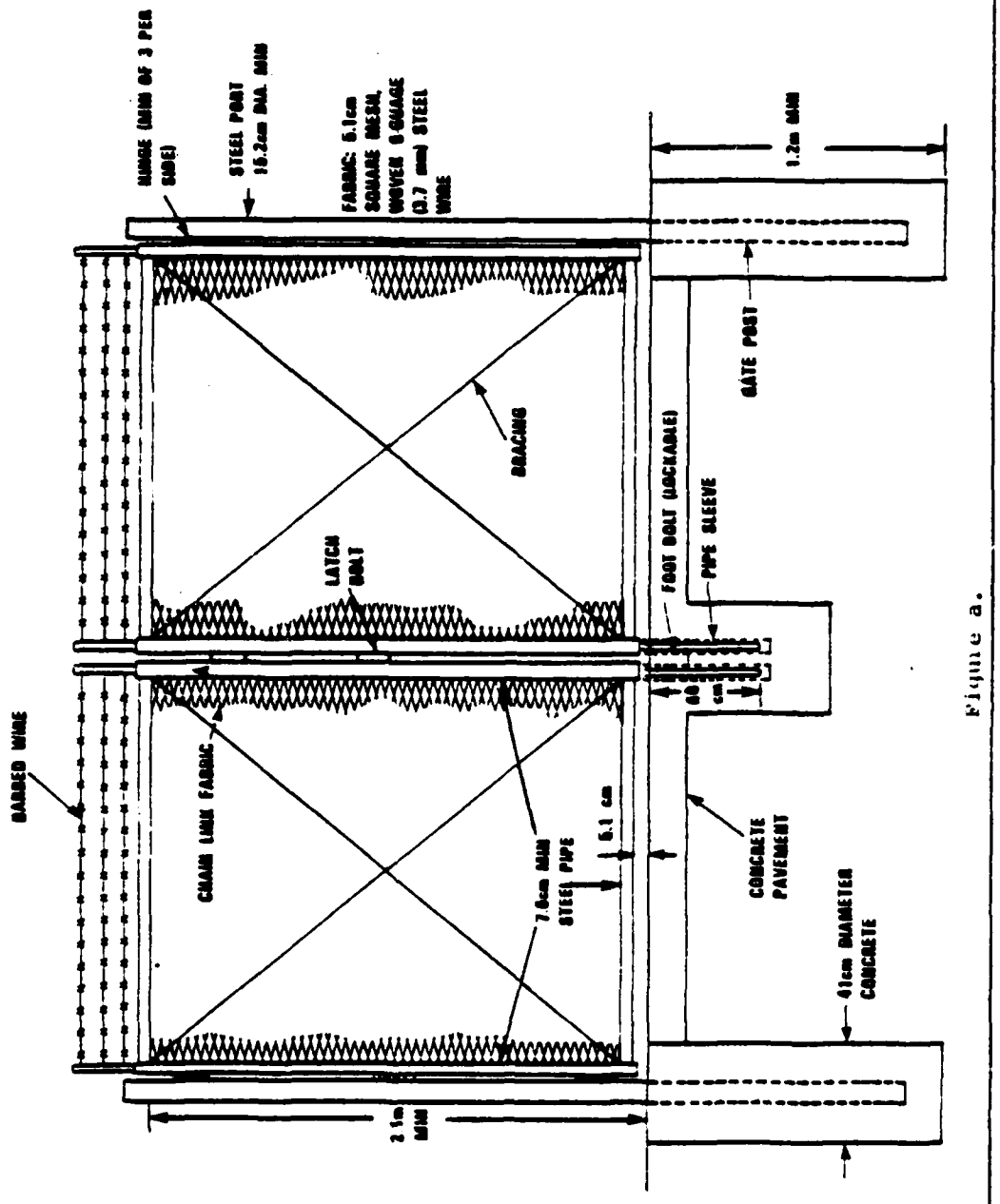


Figure a.

Figure a.

Figure 7. (Continued)

WARNING SIGNS

Description - Warning signs shall be employed at all DCS sites to deter casual intruders. The sign illustrated in Figure a is for example only. The format and content used for a sign will be a function of the location of the site and the applicable U.S. and foreign regulations.

Installation - Signs shall be made in accordance with Figure a. Warning signs shall be printed in English and the local language. The sign shall be painted white. The word WARNING shall be bright red in color. All remaining letters shall be black.

Maintenance - Warning signs shall be inspected daily at manned DCS sites and upon every visit at unmanned sites. Signs shall be inspected for damage, wear and tampering. If warning signs have

Figure 8. Warning Signs

WARNING SIGNS (Continued)

have been degraded, repairs or replacements shall be made as soon as possible.

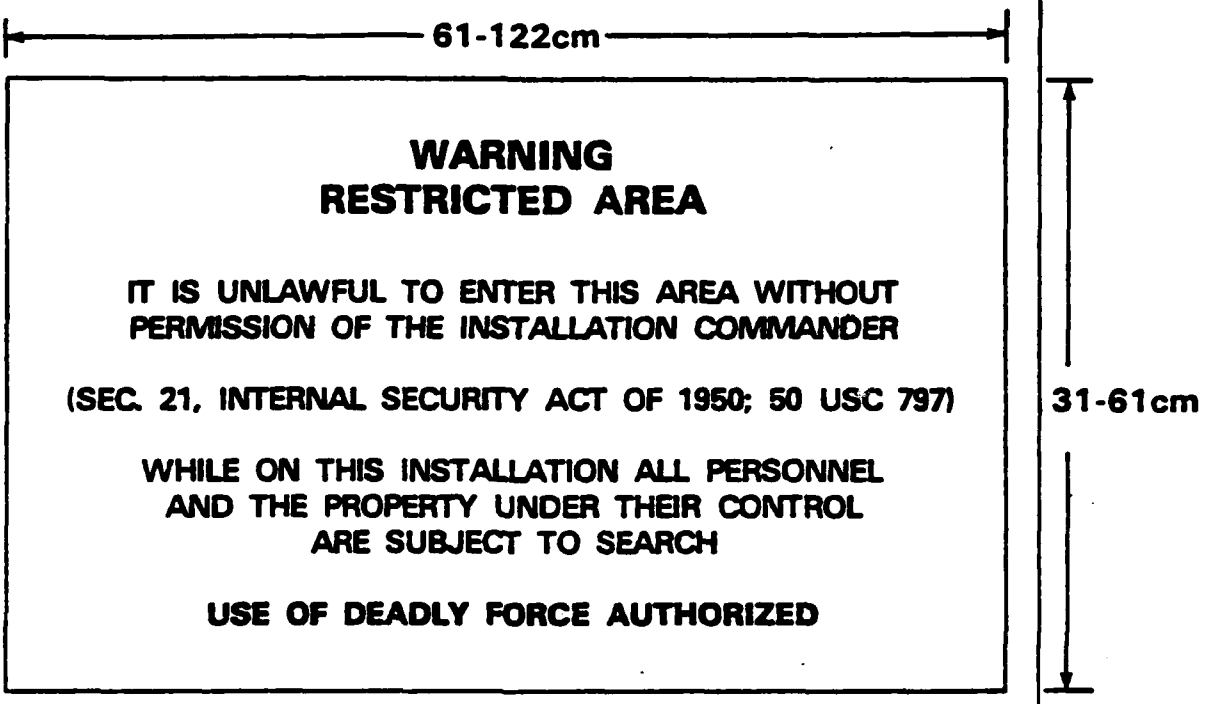


Figure a.

Note: Reflective lettering
3.7 cm min. height.

References - AFR 207-1, The Air Force Physical Security Program (U).

United States Navy Physical Security Manual, OPNAV Instruction 5510.45B, 19 April 1971.

Physical Security, U.S. Army Field Manual 19-30, March 1979.

Figure 8. (Continued)

PORTED COAX CABLE SENSOR

Description - Ported Coax Cable is an exterior surveillance sensor designed to detect and locate intruders over long perimeters. It consists of an active electromagnetic sensor buried in the ground. The Ported Coax Cable Sensor is optimally employed at large sites with perimeters up to 3.2km in length.

Operation - Ported Coax consists of two identical "leaky" coaxial cables buried in the ground parallel to each other (Figure a). A pulsed transmitter is connected to one cable transducer and a receiver is connected to a second cable transducer. The operating frequency transmitted is in the 60 MHz band (VHF). Peak transmitted power is 800mw. The pulsed energy causes a surface wave to propagate along the outside of the transmit cable. A portion of this surface wave couples into the receiver cable producing a VHF return signal at the receiver. When an intruder enters into the electromagnetic field, this coupling between the transmit and receive cables is perturbed resulting in a change in the receive signal. Due to the nature of the short VHF pulse and the design of the ported cable, the location of the intruder is determined by the time delay between the start of the transmitted pulse and the reception of the profile disturbance. This system will simultaneously detect and locate multiple intruders.

Figure 9. Ported Coax Cable Sensor

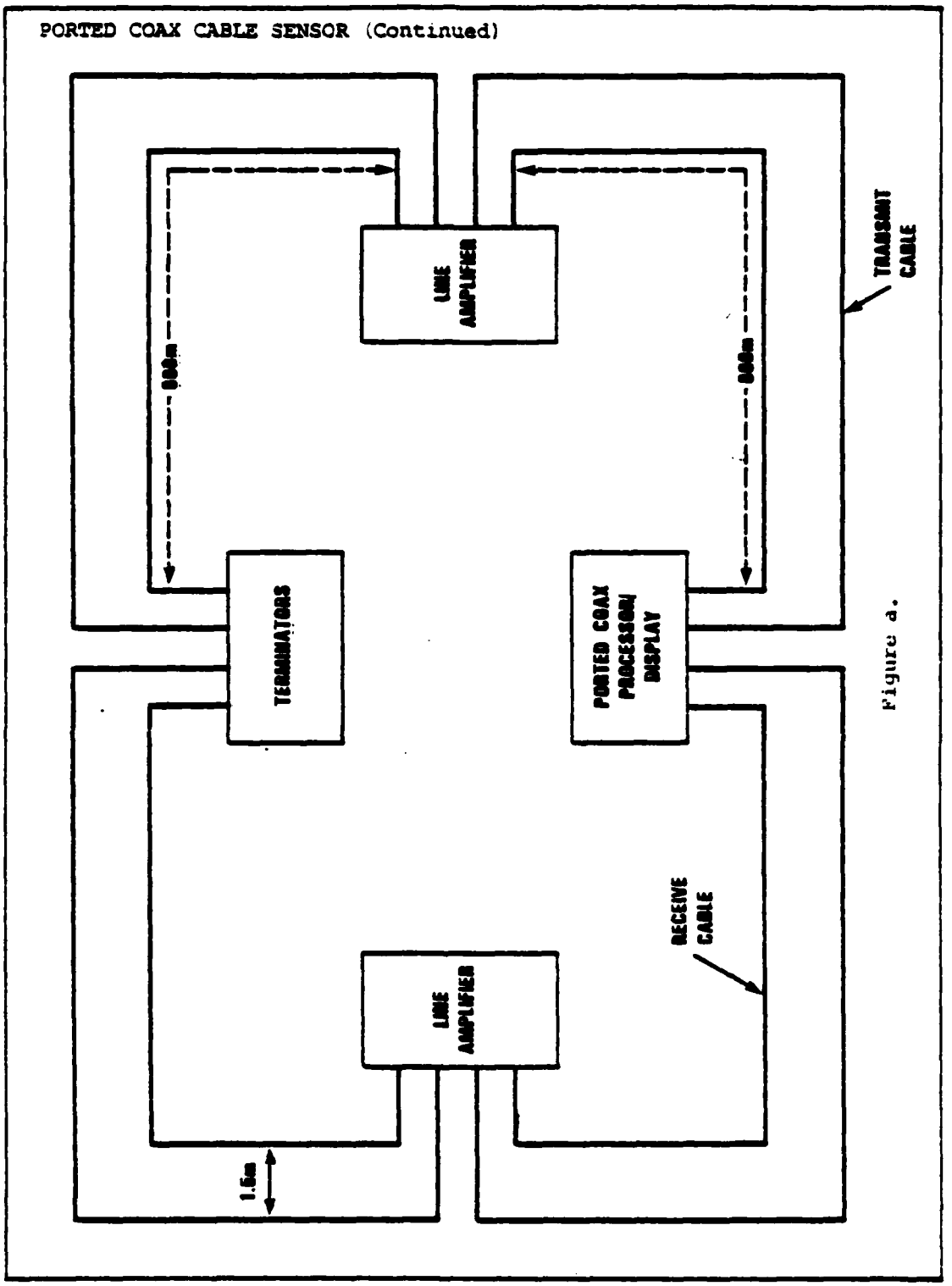


Figure a.

Figure 9. (Continued)

PORTED COAX CABLE SENSOR (Continued)

Installation - A site compatibility test is recommended prior to procurement and installation because performance characteristics are not yet established. The site compatibility test consists of the installation of a short pair of ported cables. The transmit signal is applied while received signal power is monitored for both normal and water saturated soil conditions. The purpose of the test is to determine if the system is compatible with the soil conditions found at a given site.

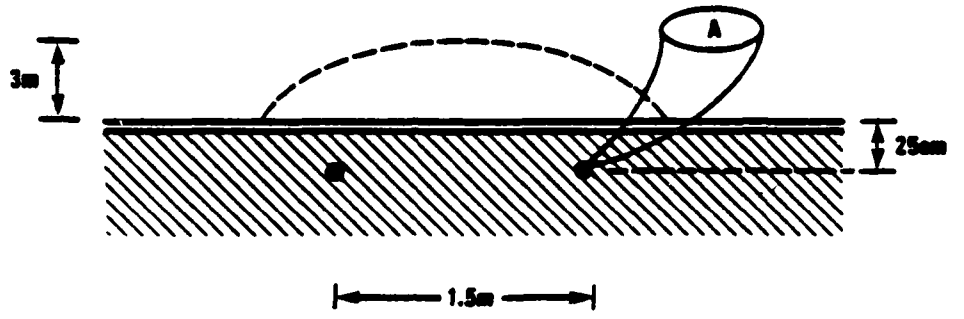
Upon actual system installation, the tolerance on both depth and cable separation is not critical. Recommended installation parameters are presented in Figure b. Uniform installation is recommended to enhance a uniform system response. The burial surface should be graded to promote water drainage. With a separation of 1.5 meters, the vertical coverage of the sensor is expected to be approximately 3m.

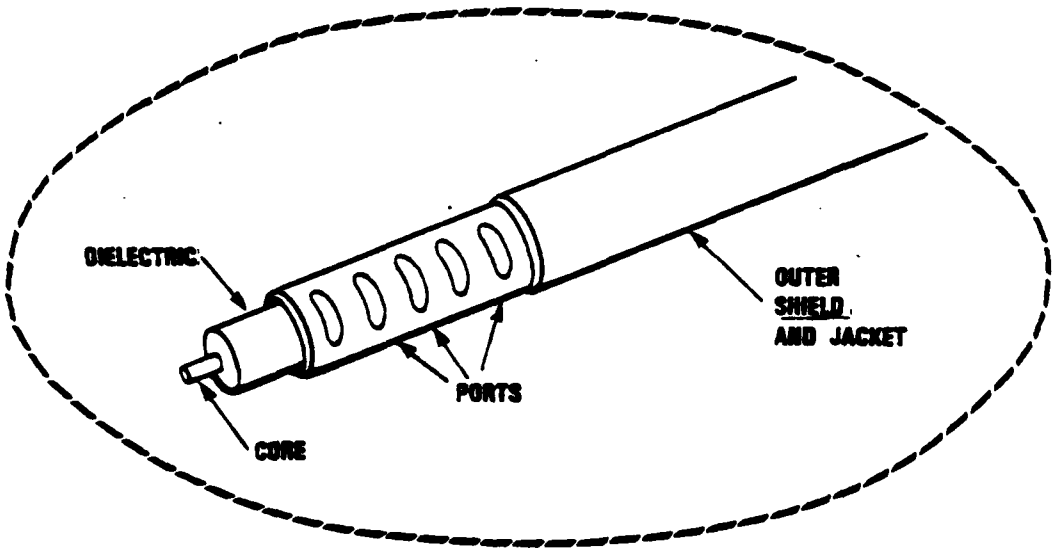
Maintenance - Department of Defense guidelines shall be followed. A daily walk-through procedure to test the detection for each 100m sector is recommended. The system contains a continuous self test feature, including manual diagnostics and external test connections.

References - Intrusion Detection Systems Handbook. Vol I and II, Sandia Laboratories, Albuquerque, NM, July 1980.

Figure 9.(Continued)

PORTED COAX CABLE SENSOR (Continued)





"A"

Figure b.

Figure 9. (Continued)

INDIVIDUAL RESOURCE PROTECTION SENSOR (IRPS)

Description - IRPS is a microprocessor based, buried line intrusion sensor for use in providing intrusion detection over short perimeter segments up to 300m in length.

Operation - IRPS consists of two identical "leaky" coaxial cables buried in the ground parallel to each other (Figure a). A transmitter is connected to one cable transducer and a receiver is connected to the second cable transducer. The transmitter cable is energized with a 60 MHz CW signal that causes a surface wave to propagate along the outside of the transmit cable. A portion of this surface wave couples into the receiver cable producing a continuous return signal at the receiver. When an intruder enters into this electromagnetic field, the coupling between the transmit and receive cables is disrupted and results in a change in the receive signal. The IRPS system offers detection only, with no indication of the exact location of the intrusion along the 300 meter length of this cable.

Installation - A site compatibility test is recommended prior to procurement and installation because performance characteristics are not yet established. The site compatibility test consists of the installation of a short pair of ported cables. The transmit signal is applied while received signal power is monitored for

Figure 10. Individual Resource Protection Sensor (IRPS)

INDIVIDUAL RESOURCE PROTECTION SENSOR (IRPS) (Continued)

both normal and water saturated soil conditions. The purpose of the test is to determine if the system is compatible with the soil conditions found at each site.

Upon actual system installation, the tolerance on both depth and cable separation is not critical. A recommended burial depth is 25cm with a cable separation of approximately 1.5 meters. Uniform installation is recommended to enhance a uniform system response. The burial surface should be graded to promote water drainage.

Maintenance - Department of Defense guidelines shall be followed. A daily walk-through procedure to test the detection for each 100m sector is recommended. The system contains a continuous self test feature, including manual diagnostics and external test connections.

References - Intrusion Detection Systems Handbook, Vols I and II, Sandia Laboratories, Albuquerque, New Mexico, July 1980.

Figure 10. (Continued)

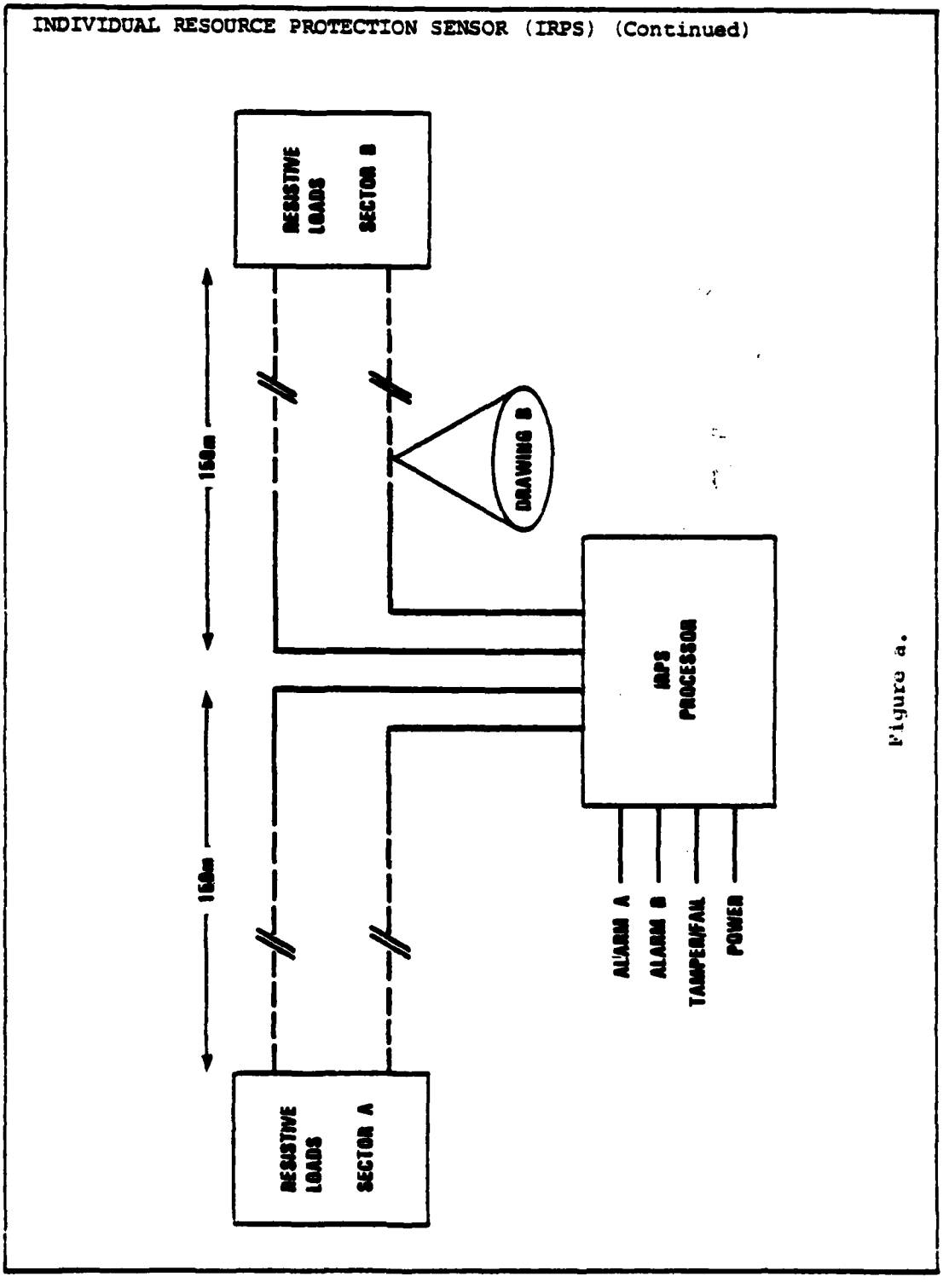


Figure 10. (Continued)

INDIVIDUAL RESOURCE PROTECTION SENSOR (IRPS) (Continued)

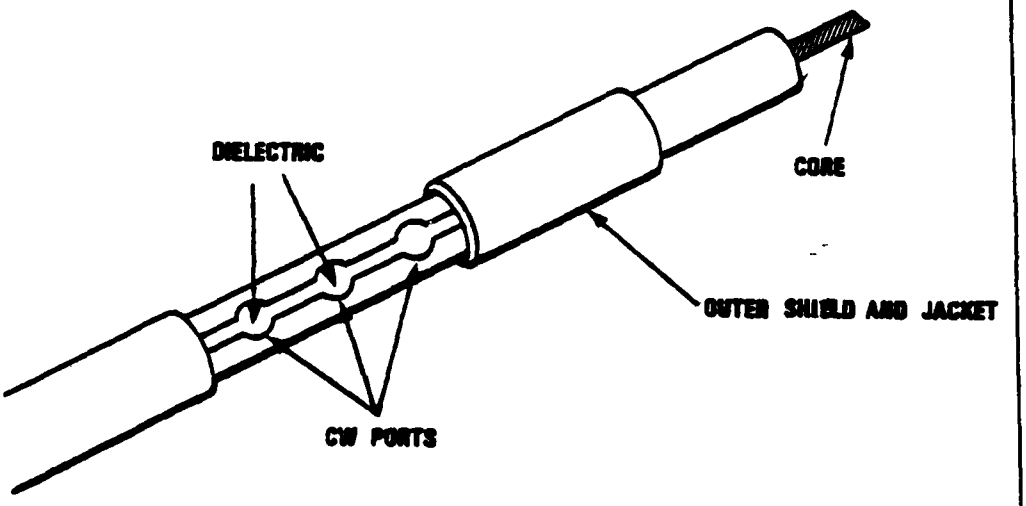


Figure b.

Figure 10. (Continued)

MILES BURIED CABLE SENSOR

Description - The MILES, Magnetic Intrusion Line Sensor, buried cable is sensitive to both magnetic and seismic disturbances and is capable of sensing crawling, walking and running targets. The MILES sensor can detect intrusions independent of the presence of ferromagnetic material. MILES is the sensory cable for the MAID/MILES sensor. MAID is the electronic processor.

Operation - The MILES cable detection capability is based on the fact that motion disturbances will either move the cable in the earth's magnetic field or strain the cable's flexible magnetic core, thus changing the core's permeability (Figure a). A disturbance will produce a signal in the sensing coil. If the response falls within a 4 Hz passband and exceeds a specified amplitude, an alarm is produced.

MILES is susceptible to false alarms from magnetic disturbances caused by lightning, power lines, buried power and signal cables and vehicle ignition noise. It is also susceptible to wind-induced ground motion and localized pressure sources such as moving vehicles, heavy equipment, and trains.

Installation - The MILES cable is installed in 100m segments. The sensor cable can follow irregular terrain. Multiple cables are

Figure 11. MILES Buried Cable Sensor

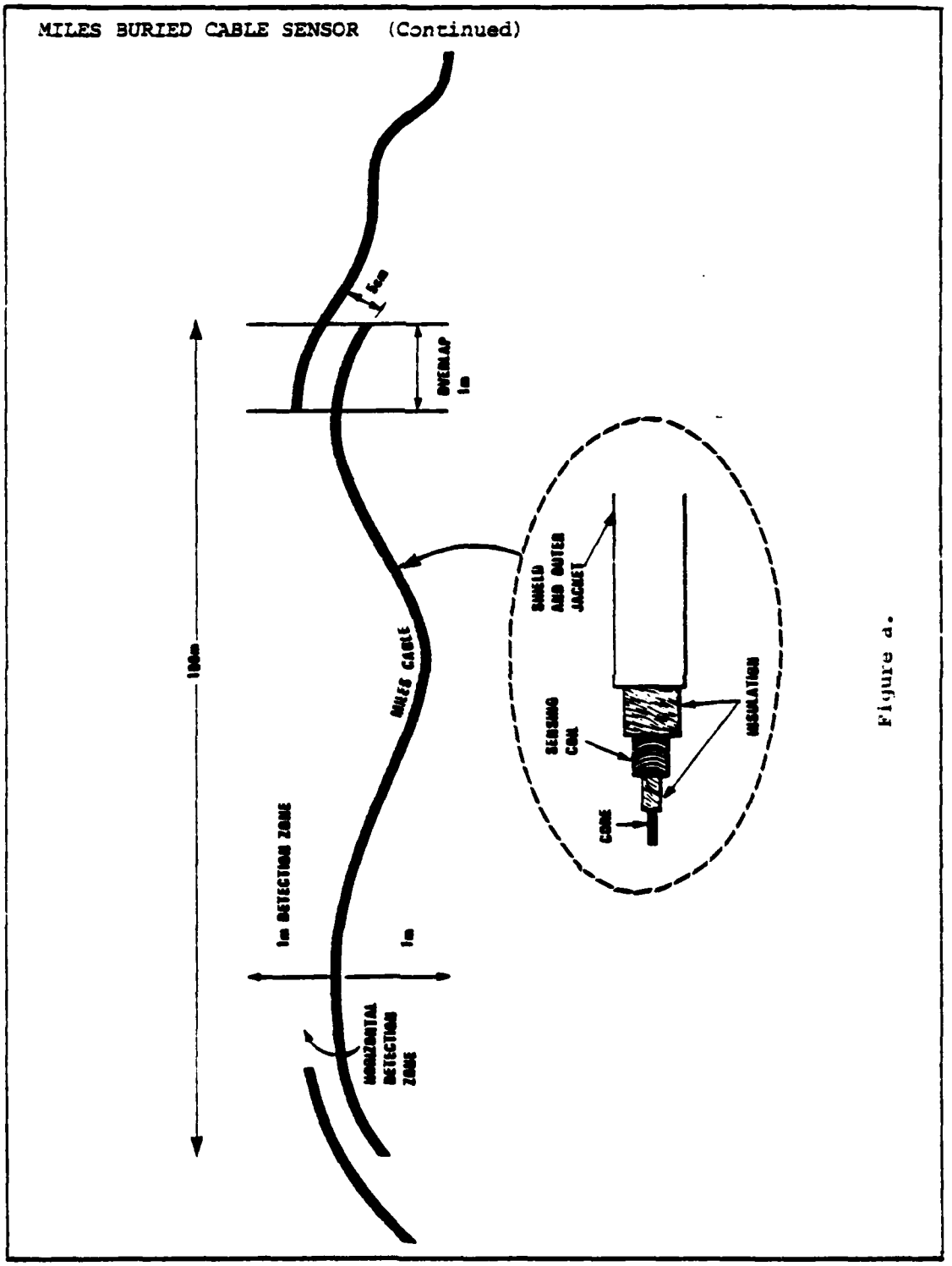


Figure 11. (Continued)

MILES BURIED CABLE SENSOR (Continued)

overlapped as shown in Figure a. For each site installation of the MILES sensor, the depth of cable burial will differ. It is necessary to perform an initial test installation at each site to determine the optimum depth. To determine the best depth, one 100m cable is cut to make as many as nine 10m lengths. It has been observed that the background noise will increase approximately in proportion to the square root of the length of the cable and that the sensitivity is independent of the length. Using these facts, in conjunction with the initial test installation, the best cable burial depth at a given site is determined.

The cable is buried in accordance with Figure b. Installation is not recommended in asphalt or concrete unless the seismic capability of the transducer can be ignored. The following table provides some specific guidelines to be followed when installing the MILES transducer near potential seismic sources.

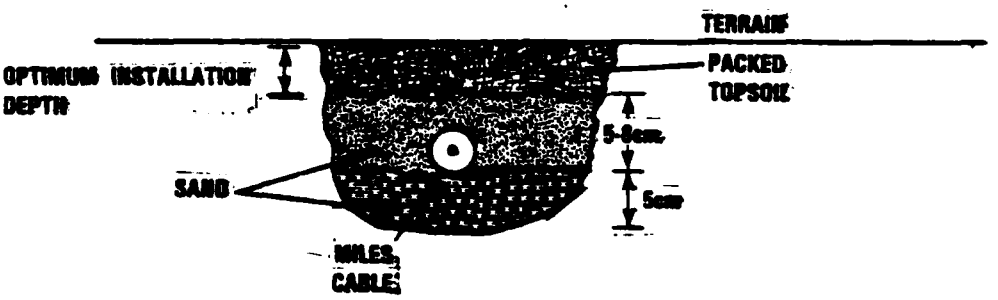


Figure b.

Figure 11. (Continued)

MILES BURIED CABLE SENSOR (Continued)

Table of Guidelines

Source	Recommended Separation
Chain link fence	3 m
Power poles	equal to height of pole
Guy wires for power poles	6 m
Tree drip lines	9 m
Buildings housing machinery	6 m
Roads with approx. 85 km/h traffic or heavy trucks	100 m
Roads with approx. 16 km/h traffic and no heavy trucks	10 m

Maintenance - The self test feature of the MAID/MILES sensor shall be exercised at random intervals not to exceed one hour. Maintenance of the terrain, such as removing vegetation or filling eroded areas shall be performed as required. If the transducer is suspected of degraded performance, testing shall be initiated. Periodic performance testing is also recommended.

References - Intrusion Detection Systems Handbook, Vols. I and II, Sandia Laboratories, Albuquerque, New Mexico, July 1980.

Figure 11. (Continued)

BISTATIC MICROWAVE SENSORS

Description - Bistatic microwave sensors consist of an X-band source transmitting over a clear area of approximately 60 m to a receiver (Figure a). The transmitted signal is modulated at an audio frequency to form an amplitude sensitive beam breaking system. Multiple sensors are required to cover large perimeters and corners.

Operation - A bistatic microwave sensor is a line-of-sight device. The volume encompassed by the sensor is depicted in Figure b. The transmit antenna propagates a modulated signal toward the receive antenna. Terrain features, mounting height of the antennas, phase relationships and other characteristics determine the received signal strength and the offset which is the distance on the ground relative to the transmitter or receiver through which an intruder can crawl without detection. With an unauthorized entry into the detection zone, a portion of the transmitted energy will be deflected away from the receive antenna resulting in a change in signal strength and an alarm sequence will be initiated.

The microwave sensor is susceptible to the crawling intruder and to tampering. In addition, the area between the transmitter

Figure 12. Bistatic Microwave Sensors

BISTATIC MICROWAVE SENSORS (Continued)

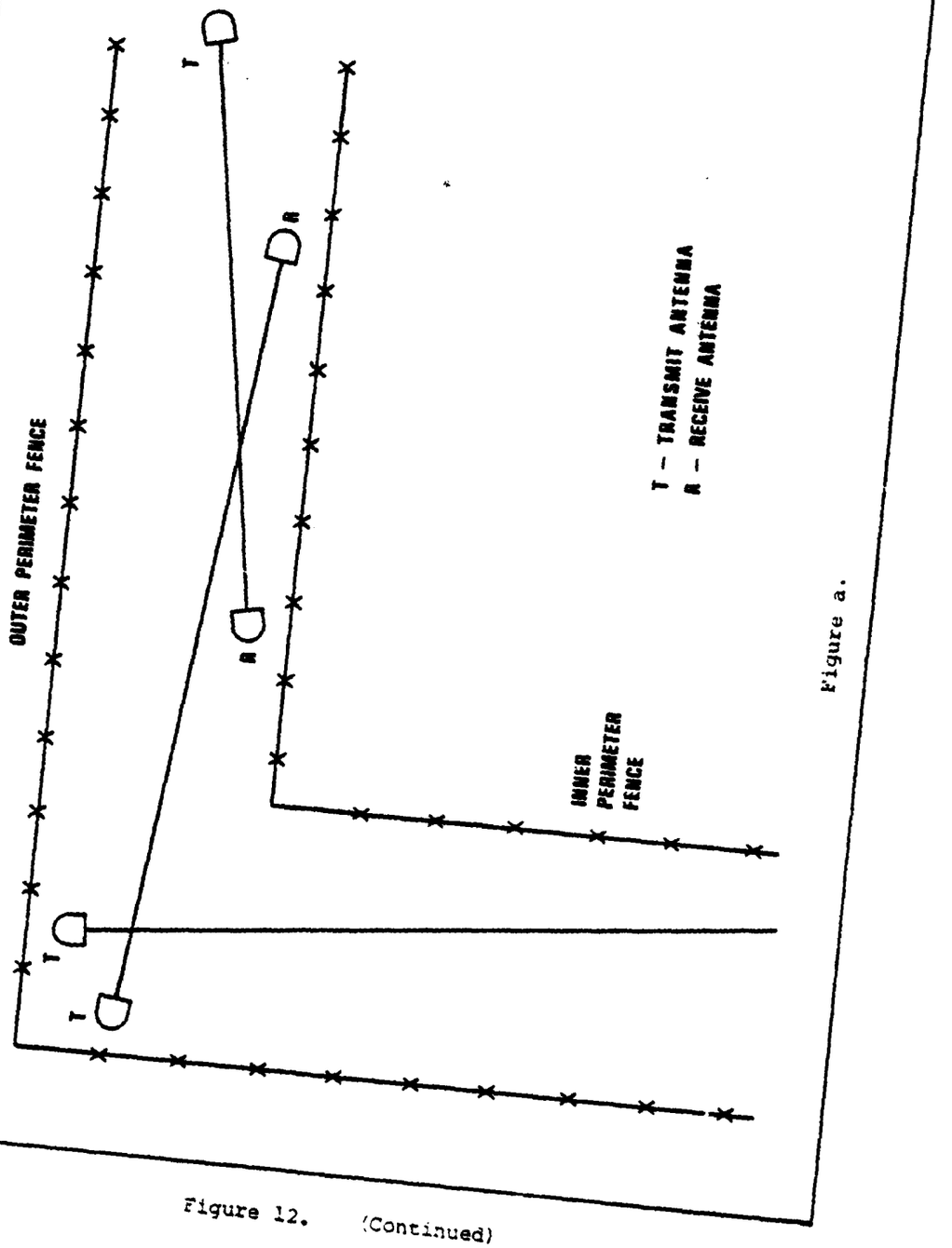


Figure a.

Figure 12. (Continued)

BISTATIC MICROWAVE SENSORS (Continued)

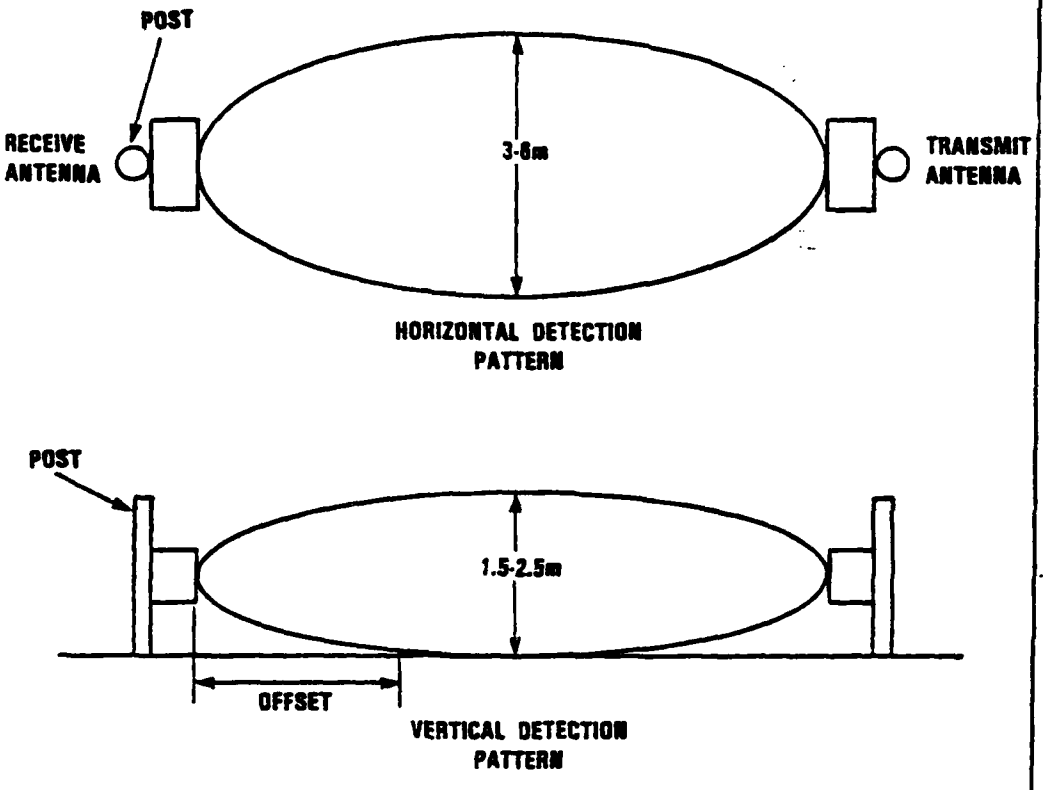


Figure b.

Figure 12. (Continued)

BISTATIC MICROWAVE SENSORS (Continued)

and receiver must be kept clear of all obstructions including grass or vegetation to maintain a suitable false alarm rate.

Installation - Prior to installation of a bistatic microwave sensor the coverage area shall be prepared in the following manner:

- Grass and weeds shall be controlled by soil sterilization or surfacing.
- Raised features shall be graded and depressions filled in order that no site discontinuities over 3 cm in size exist.
- The surface may be dirt, gravel, asphalt, concrete, or any combination as long as heavy rainfall will not cause errosion of the surface.
- Structures such as towers, buildings, and fences shall be separated sufficiently from the microwave beam center line so as to not cause reflections which would degrade the system performance.
- If deep snow is a problem at the site, snow fencing shall be employed.

The installation of the sensor mounting post requires a fixed location steel pipe embedded in concrete. The system requirements, such as number of sensors to be mounted, will dictate pipe diameter and length. The pipe shall be installed as near to vertical as

Figure 12. (Continued)

BISTATIC MICROWAVE SENSORS (Continued)

possible. All exposed signal lines shall be enclosed in conduit. All connecting signal wires shall be run underground in conduit.

Final elevation and azimuth alignment shall be carried out as recommended by the particular sensor manufacturer.

Maintenance - Periodic testing and maintenance is necessary to ensure system reliability and performance. A regular complete maintenance test shall be performed when the system is suspected of performance degradation or every six months.

References - Intrusion Detection Systems Handbook, Vols. I and II, Sandia Laboratories, Albuquerque, New Mexico, July 1980.

Figure 12. (Continued)

TAUT WIRE FENCE

Description - A continuous taut wire fence shall be employed inside the perimeter fence of all DCS sites to deter casual intruders and to sense intrusions.

Installation - Taut wire fence shall be constructed in accordance with Figure a. The sensor post shall be located approximately midway between the anchor posts. Intermediate slider posts shall be located at 3m maximum intervals between the sensor and anchor

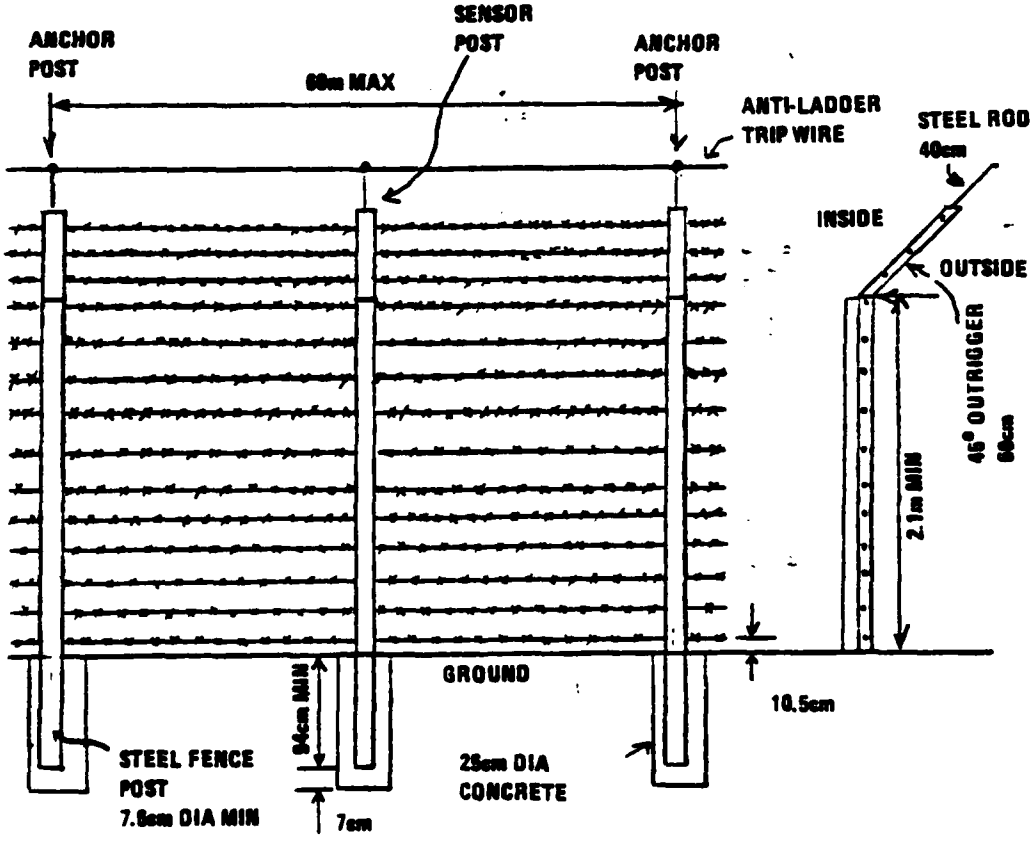


Figure a

Figure 13 Taut Wire Fence

TAUT WIRE FENCE (Continued)

posts. The taut wire sensor shall be mounted to the sensor post in accordance with Figure b. The cumulative change in fence alignment on

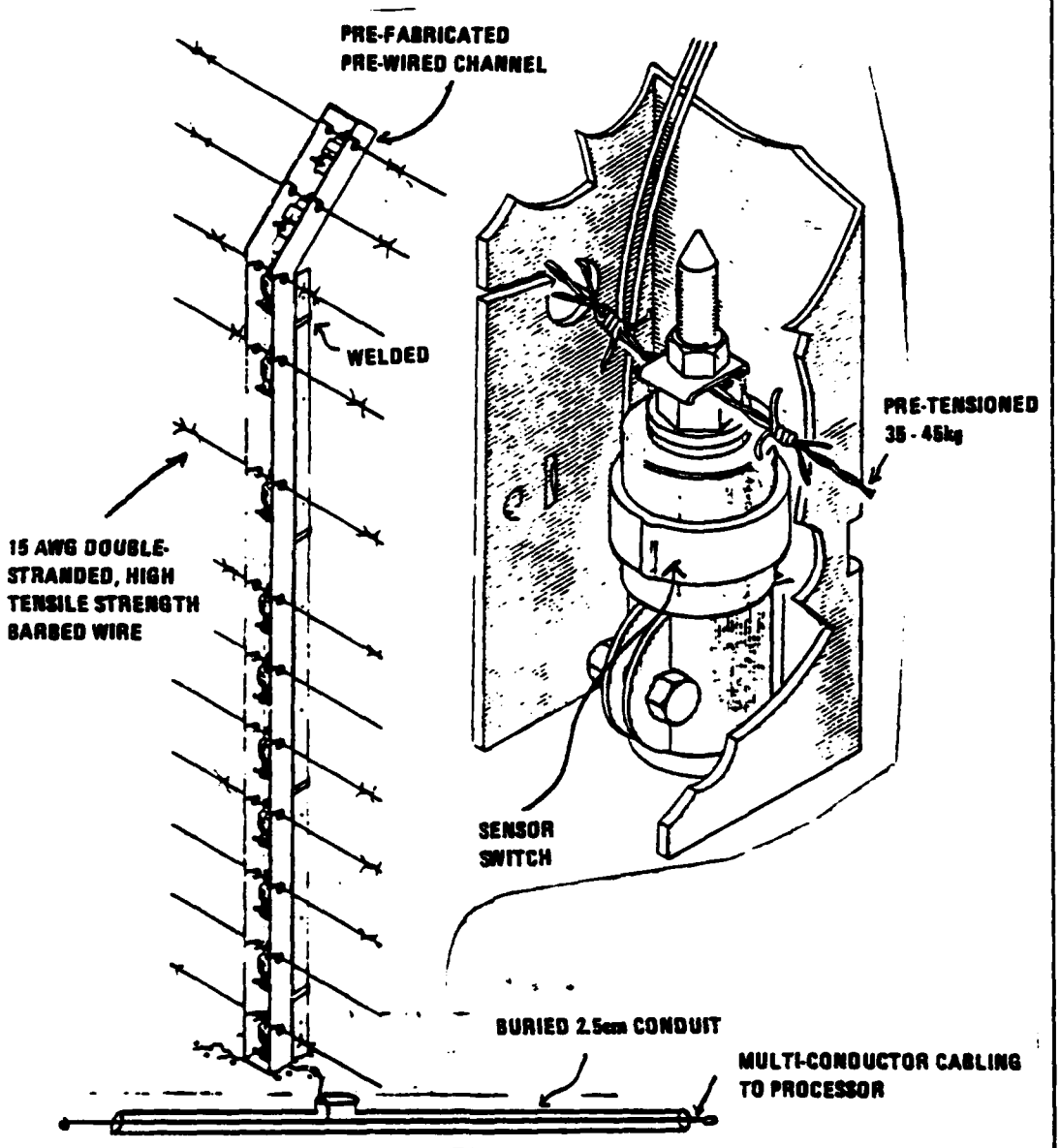


Figure b

Figure 13 (Continued)

TAUT WIRE FENCE (Continued)

each side of a sensor post shall not exceed 15 degrees. The ground path along the taut wire fence shall be clear and graded.

Maintenance - Simulated intrusion tests shall be performed routinely. Each sensor switch shall be unclamped at no longer than 6 month intervals to permit the sensor switch to return to its neutral position. The taut wire fence shall be inspected daily at manned DCS sites and upon every visit to unmanned sites. Fences shall be inspected for damage, wear or tampering, erosion of soil, loosened fittings or growth of vegetation in cleared areas. Necessary repairs or replacements shall be made as soon as possible.

References - Intrusion Detection Systems Handbook, Vols. I and II, Sandia Laboratories, Albuquerque, New Mexico, July 1980.

Figure 13 (Continued)

TAUT WIRE FENCE GATE

Description - A DCS site shall employ a single leaf gate in taut wire fences for authorized access of personnel and maintenance vehicles.

Installation - Taut wire fence gates shall be constructed in accordance with Figure a. All bracing shall be mounted inside the gate

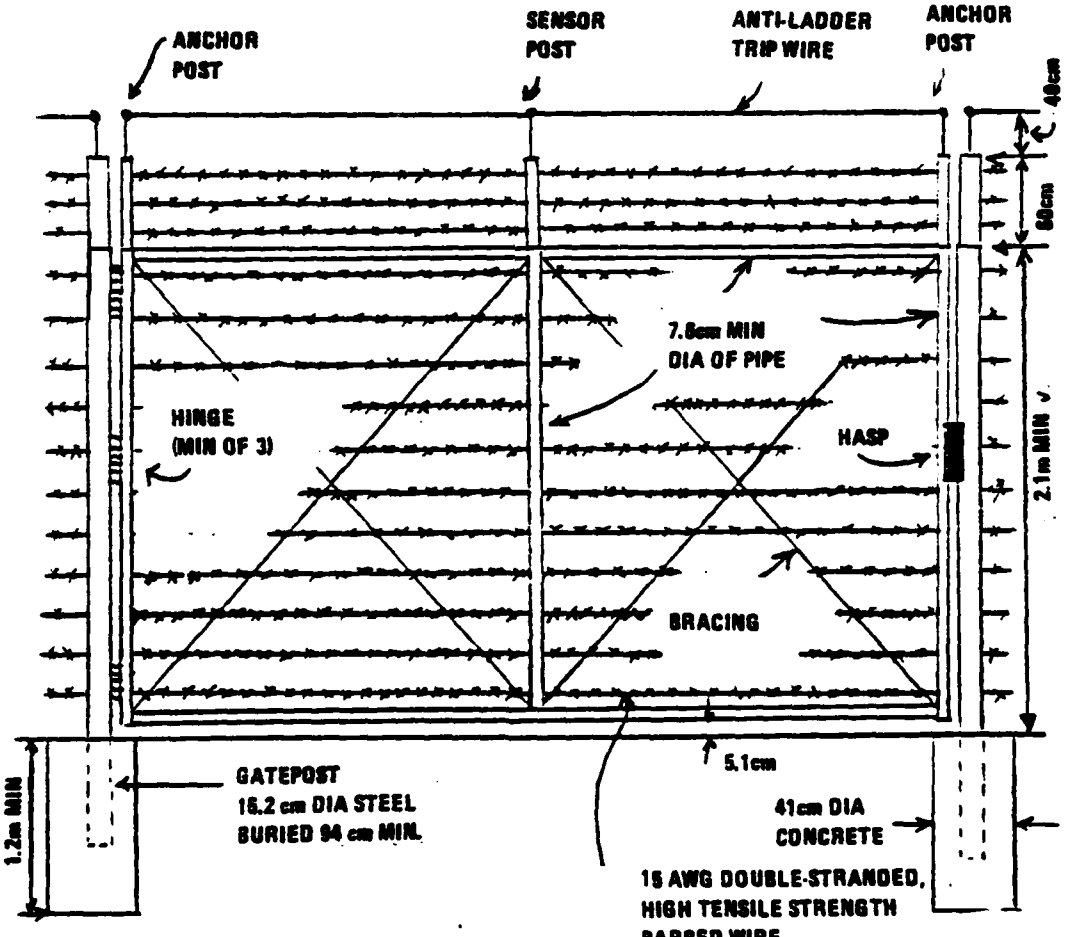


Figure a

Figure 14 Taut Wire Fence Gate

TAUT WIRE FENCE GATE (Continued)

fabric. All gate hardware shall be peened and welded to prevent removal. Gates shall be topped in the same manner as the adjacent fencing unless that configuration interferes with the operation of the gate in which case the outrigger may be replaced with a single vertical arm. The sensor post shall be located approximately midway between the anchor posts. Intermediate slider posts shall be located at 3m maximum intervals between the sensor and anchor posts.

Maintenance - Simulated intrusion tests shall be performed routinely. Each sensor switch shall be unclamped at no longer than 6 month intervals to permit the sensor switch to return to its neutral position. The taut wire fence shall be inspected daily at manned DCS sites and upon every visit to unmanned sites. Fences shall be inspected for damage, wear or tampering. Necessary repairs or replacements shall be made as soon as possible.

References - Intrustion Detection Systems Handbook, Vols I and II, Sandia Laboratories, Albuquerque, New Mexico, July 1980.

Figure 14 (Continued)

GATE HOUSE

Description - Gate houses shall be erected at all DCS manned sites where a guard is posted for site entry control.

Installation - Gate houses shall be armored to provide protection from small arms fire. A secure communications link shall be implemented between the gate house and appropriate site personnel. A duress alarm shall also be provided in the gate house. A typical gate house is depicted in Figure a. The gate house shall be located inside the inner fence adjacent to the gate.

Maintenance - Gate houses shall be inspected periodically for damage or wear. Necessary repairs or replacements shall be made as soon as possible.

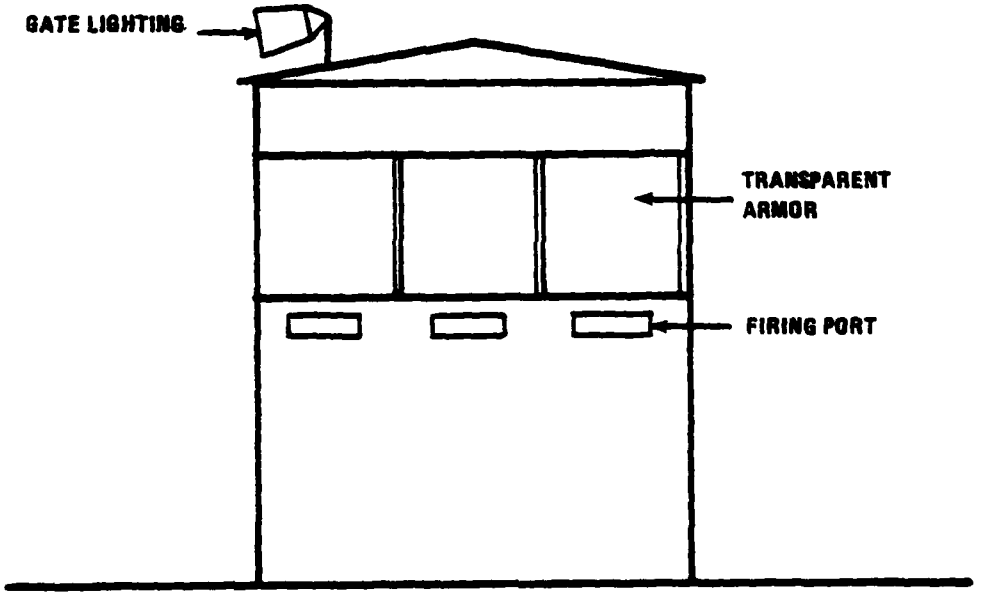


Figure a.

Figure 15 Gate House

GATE HOUSE (Continued)

References - Physical Security, U.S. Army Field Manual 19-30, March, 1979.

Figure 15 (Continued)

CCTV SYSTEM

Description - The CCTV system shall consist of television cameras positioned within the site compound to permit visual assessment of intrusion alarms and enhance site entry control.

Installation - The television cameras shall be mounted on a vibration free light pole in accordance with Figure a. Camera mounting height, tilt angle, and lighting requirements depend upon the field of view to be covered and shall be determined in accordance with DOD recommendations. A typical camera array for site entry control and alarm assessment is depicted in Figure b. The field of view shall be chosen such that the time from initial alarm to operator assessment is less than the time for an intruder to penetrate beyond

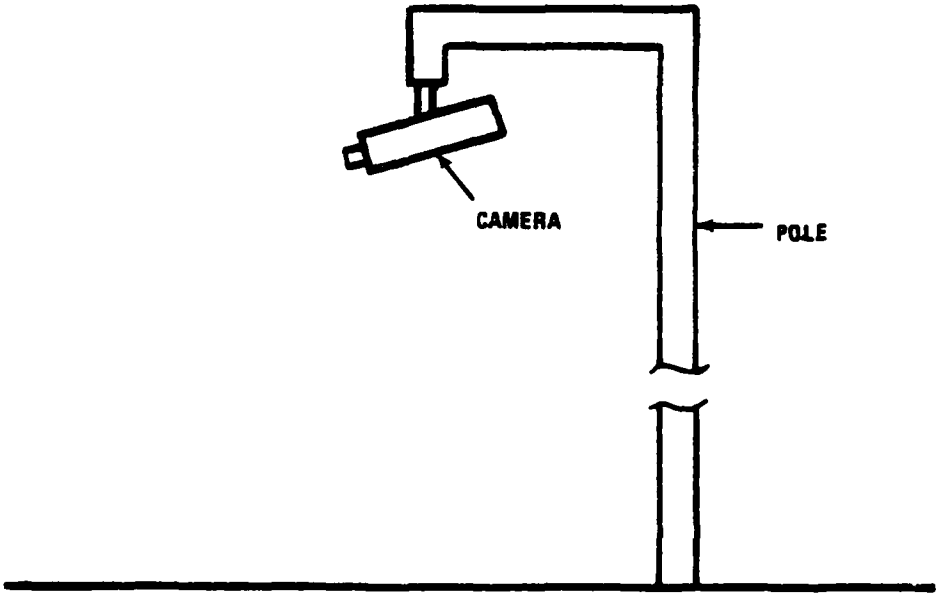


Figure a.

Figure 16. CCTV System

CCTV SYSTEM (Continued)

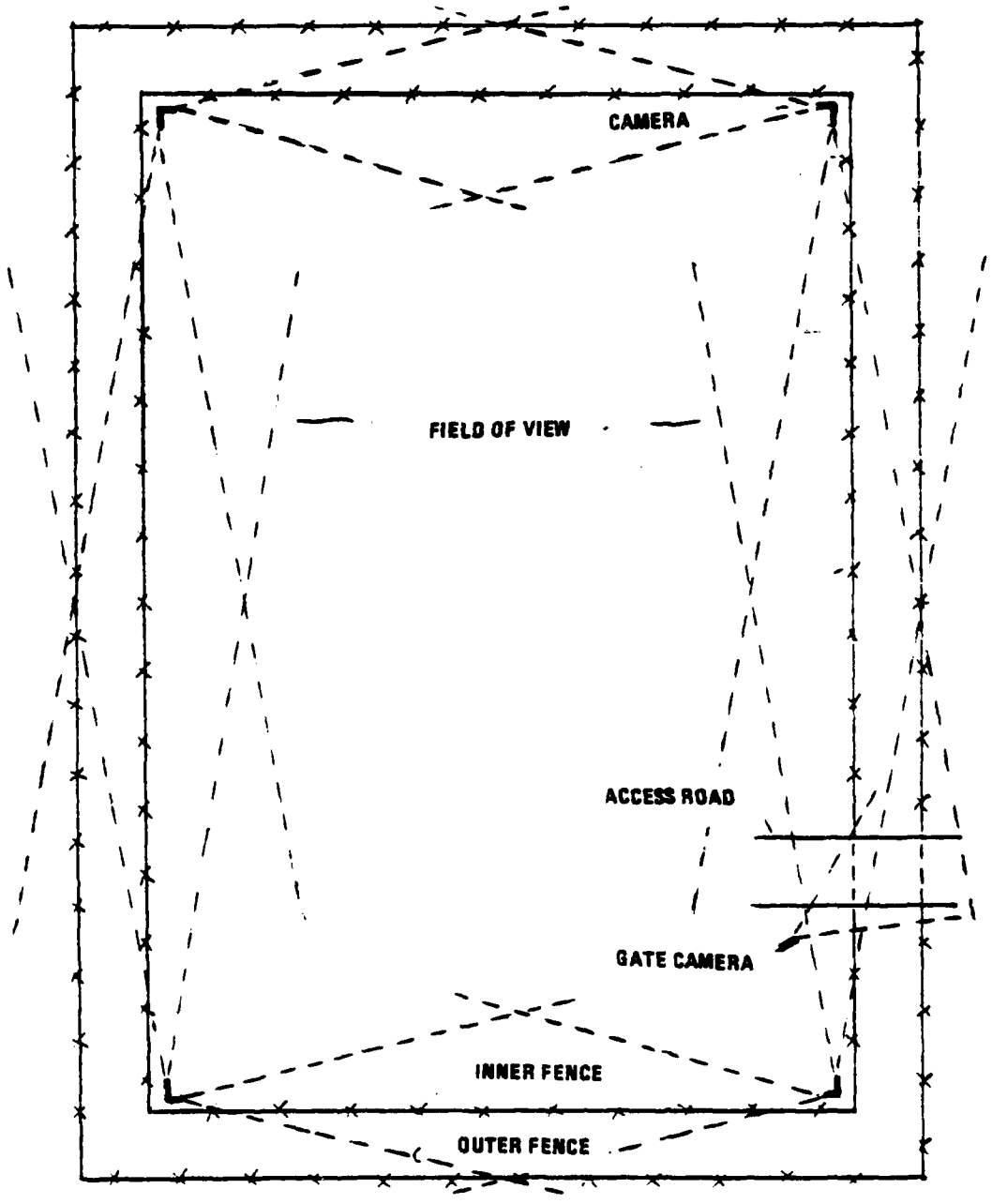
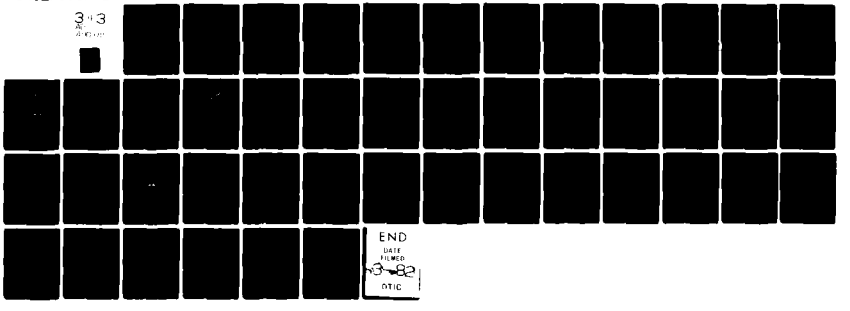
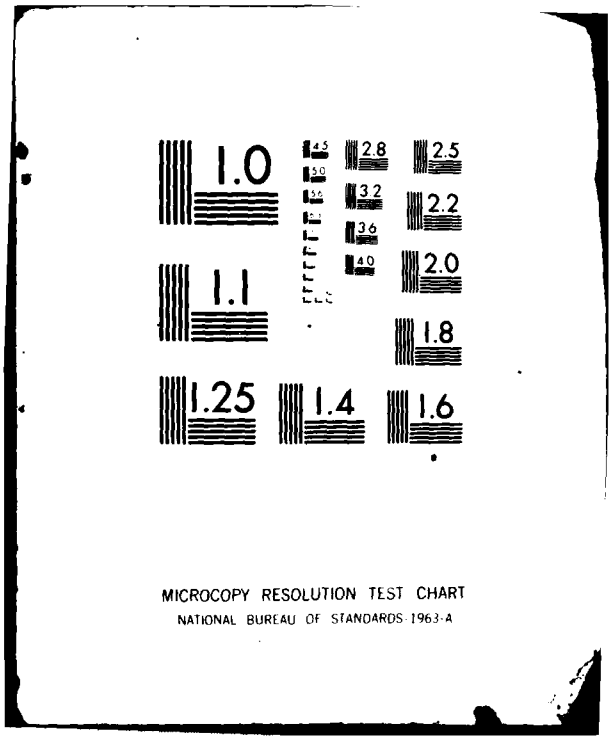


Figure b.

Figure 16.(Continued)

AD-A110 011 BOOZ-ALLEN AND HAMILTON INC BETHESDA MD F/G 13/12
DEVELOPMENT OF A DRAFT PHYSICAL SECURITY MILITARY STANDARD FOR --ETC(U)
DEC 81 H A GIESKE, M G OTTEN, D C PIERCE DAAK21-81-C-0095
UNCLASSIFIED HDL-CR-81-0095-1 NL




1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

CCTV SYSTEM (Continued)

the field of view. Video monitors shall be manned continuously to minimize assessment time.

Maintenance - Video performance shall be monitored continuously for degradation. If degradation occurs the system shall be repaired immediately by the substitution of on-site spares for the degraded units. Camera housings shall be cleaned periodically or at the first sign of decreased visibility. The drive units shall be tested on a daily basis.

References - Intrustion Detection Systems Handbook, Vol II, Sandia Laboratories, Albuquerque, New Mexico, July 1980.

Figure 16. (Continued)

GUARD TOWER

Description - Guard towers on manned sites shall be so located to enhance visual assessment of alarms and provide fire support in the event of an armed attack.

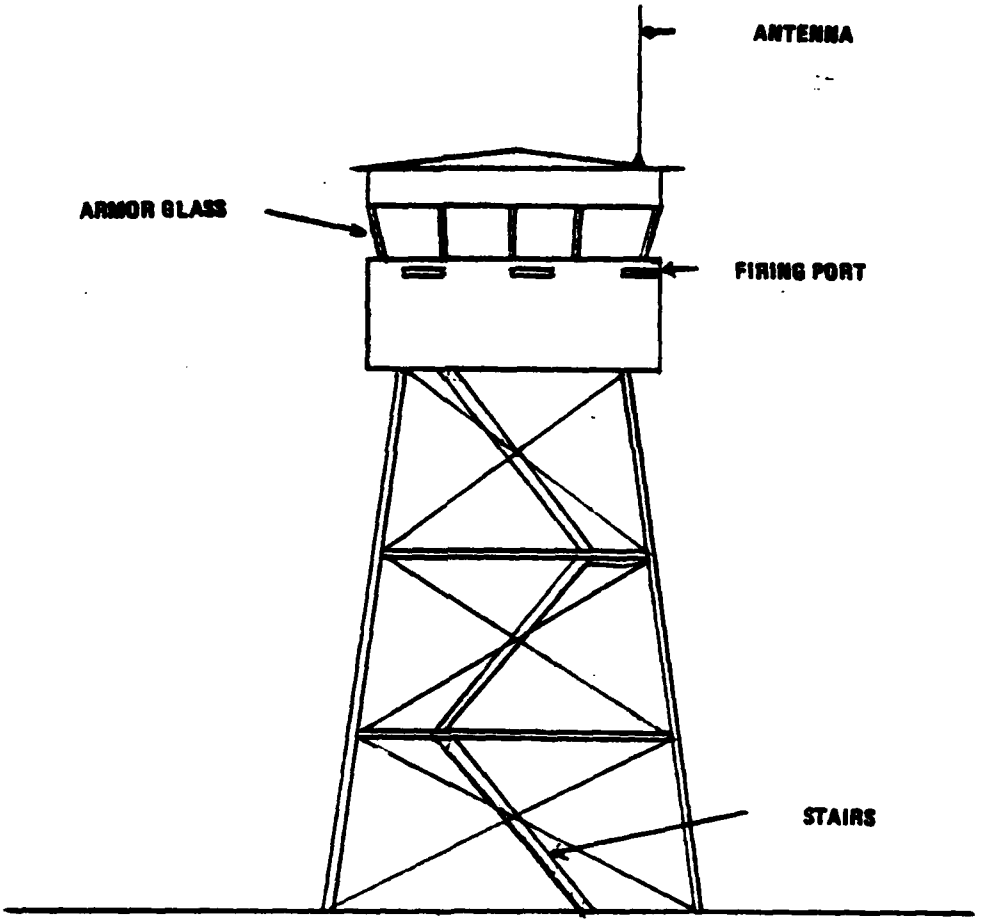


Figure a

Figure 17. Guard Tower

GUARD TOWER (Continued)

Installation - A typical guard tower is depicted in Figure a. Guard tower height and location is site dependent and shall be chosen to maximize the field of view of the site compound and perimeter. The guard tower shall be hardened to protect the occupants from attack. Sensor display shall be located within the guard tower to optimize alarm assessment. Secure communications links shall be maintained between the tower and appropriate site personnel.

Maintenance - The guard tower shall be inspected periodically for degradation of the tower structure.

References - Physical Security, U.S. Army Field Manual 19-30, March 1979.

Figure 17. Guard Tower

LIGHTING

Description - DCS sites shall employ perimeter lighting, area lighting, entry point lighting and special purpose lighting as required.

Installation - Lighting shall be constructed in accordance with Figure a. The intensity of illumination shall be as specified in the following table.

Location	Intensity on Horizontal Plane at Ground Level (lux)
Perimeter clear zone	4
Entry point	16
Inner area	2

Maintenance - Periodic inspections shall be made of all electrical circuits to replace or repair worn parts, tighten connections, and check insulation. Luminaries shall be kept clean and properly aimed.

References - Physical Security, U.S. Army Field Manual 19-30, March 1979.

Figure 18 Lighting

LIGHTING (Continued)

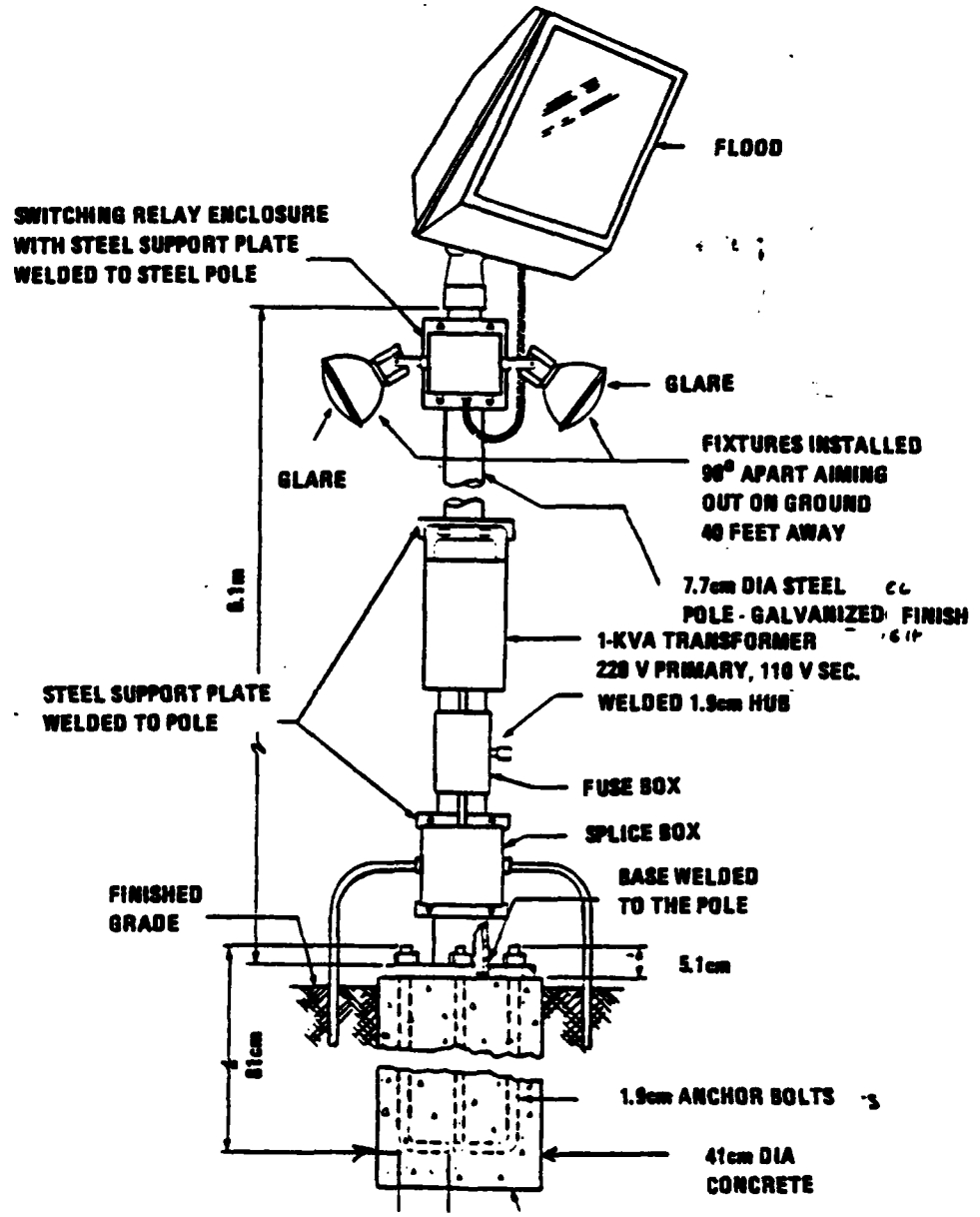


Figure a.

Figure 18 (Continued)

GABION

Description - All buildings on unmanned DCS sites shall be surrounded by a gabion to protect the building against standoff weapon fire.

Installation - The gabion shall consist of two concentric chain link fences, constructed in accordance with Figures a and b, filled with rock 5-16cm in diameter. The chain link fence shall be constructed in accordance with Figure a with additional bracing at corners and end posts. All posts and bracings shall be mounted inside the fence fabric. Adjacent posts of the inner and outer chain link fences shall be connected with wire straps for rigidity.

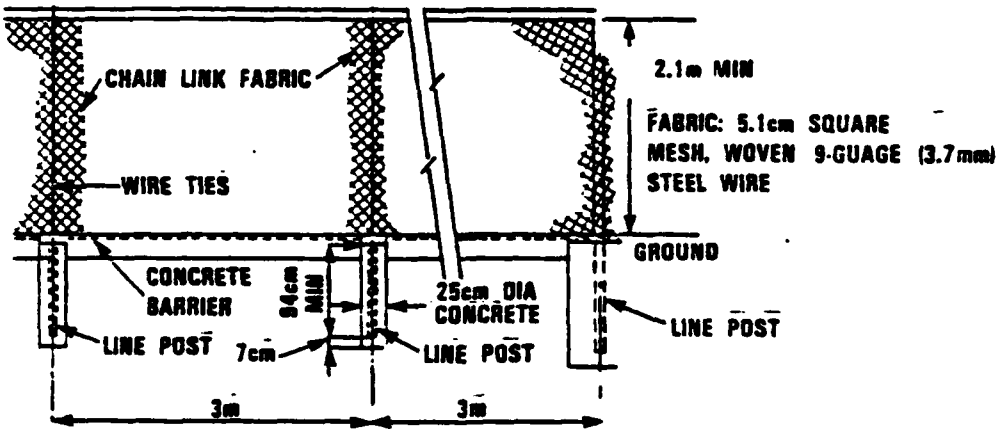


Figure a

Figure 19 Gabion

GABION (Continued)

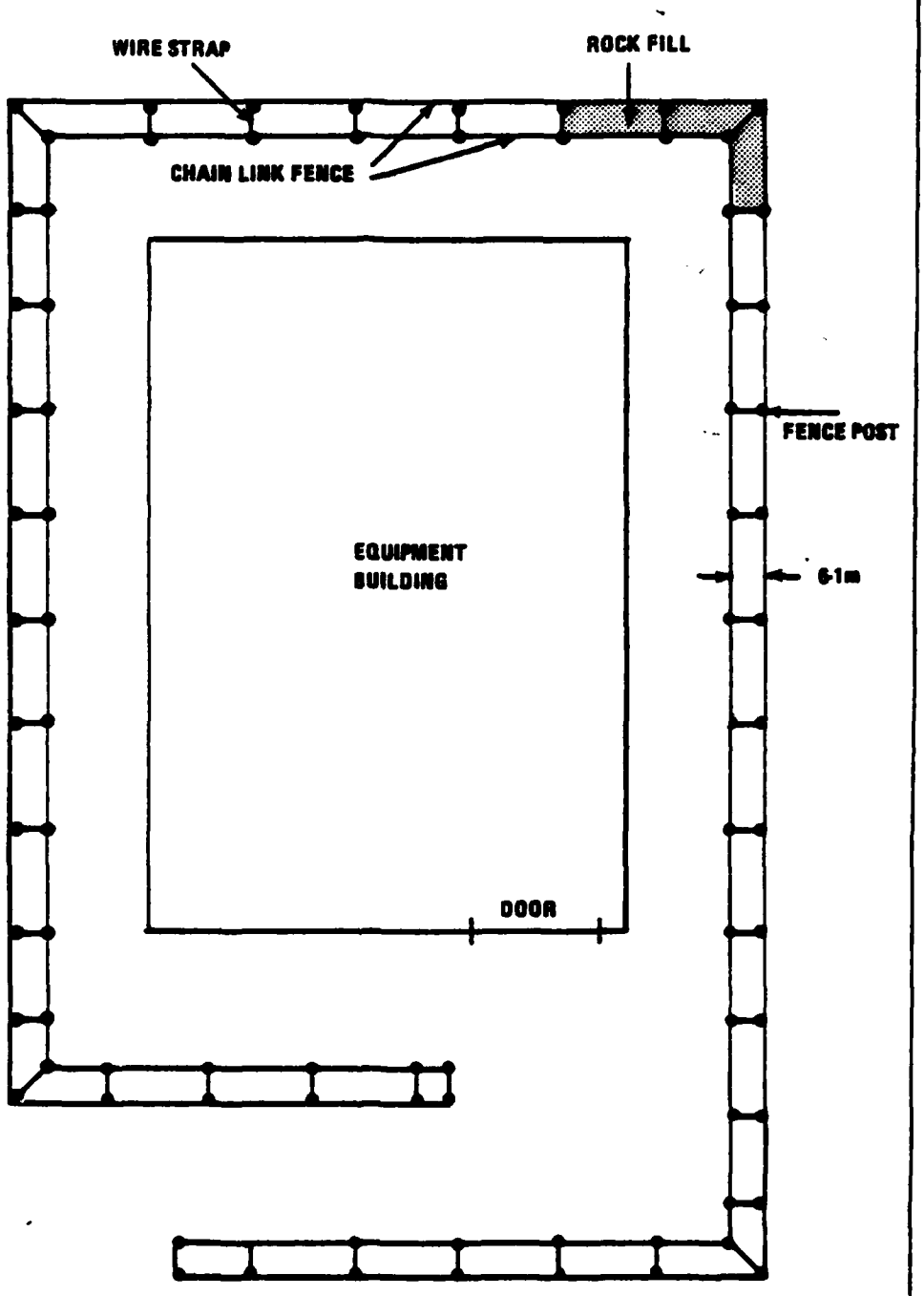


Figure b

Figure 19 (Continued)

GABION (Continued)

Maintenance - Gabions shall be inspected upon every visit to unmanned sites. Gabions shall be inspected for damage, wear or tampering, erosion of soil, or loosened fittings. Necessary repairs or replacements shall be made as soon as possible.

References - Physical security, U.S. Army Field Manual 19-30, March 1979.

U.S. Federal Specification RR-F-191/1 Type I.

Figure 19 (Continued)

NEW FACILITY DESIGN

Description - New DCS facilities shall be designed so as to incorporate all equipments and waveguides within a spun concrete tower and, where possible, an underground vault.

Installation - If the terrain is suitable, new DCS facilities shall be constructed in accordance with Figure a. If the terrain will not permit a buried vault, a DCS facility shall be constructed in accordance with Figure b.

Maintenance - Routine maintenance procedures commensurate with those conducted for existing buildings and towers shall be adopted.

Reference - Construction Design Criteria for the Protection of Air Force Operated DCS Sites, U.S. Air Force, HQ AFCS/DEO, October 1979.

Figure 20 New Facility Design

NEW FACILITY DESIGN (Continued)

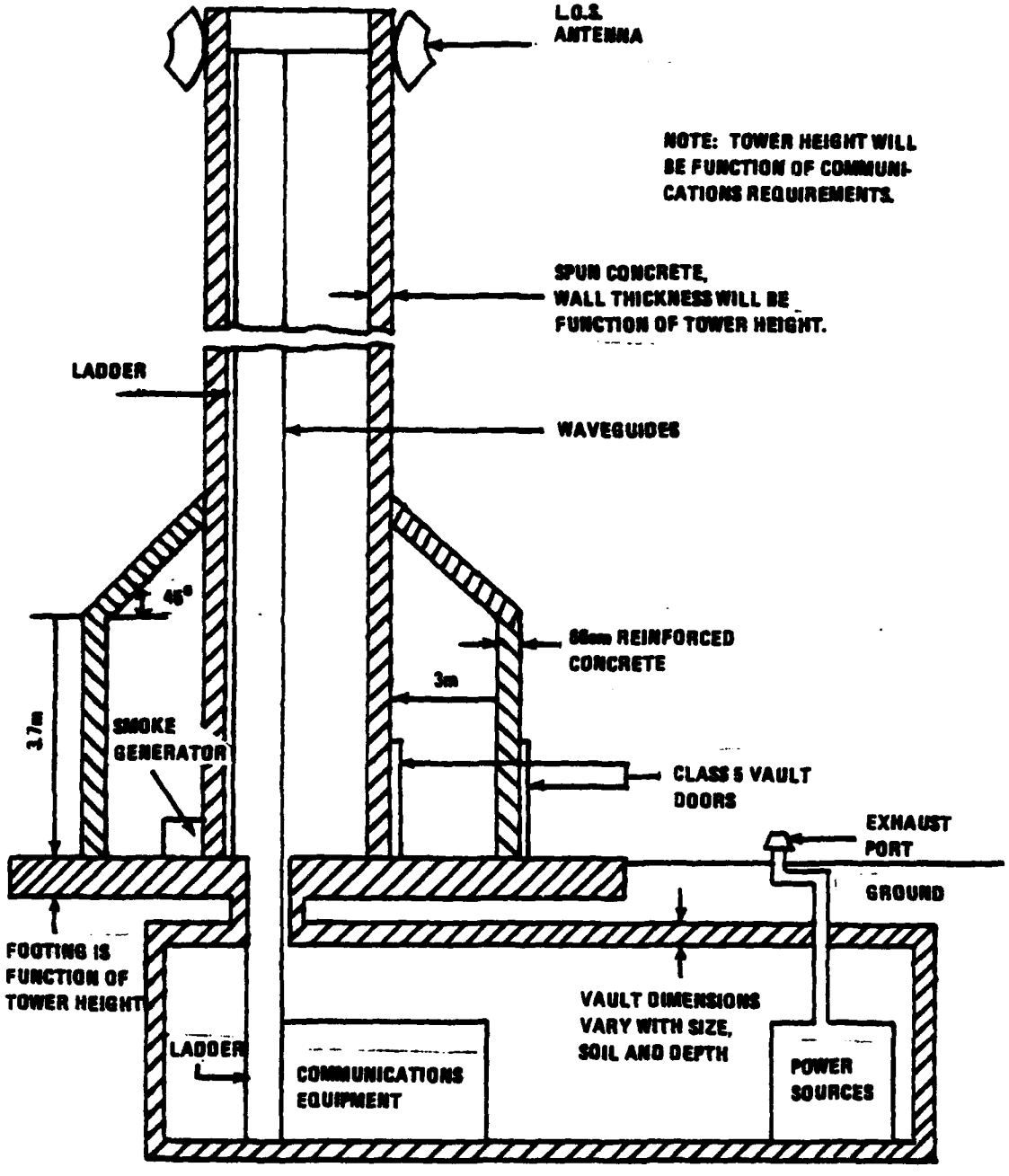


Figure a.

Figure 20. (Continued)

NEW FACILITY DESIGN (Continued)

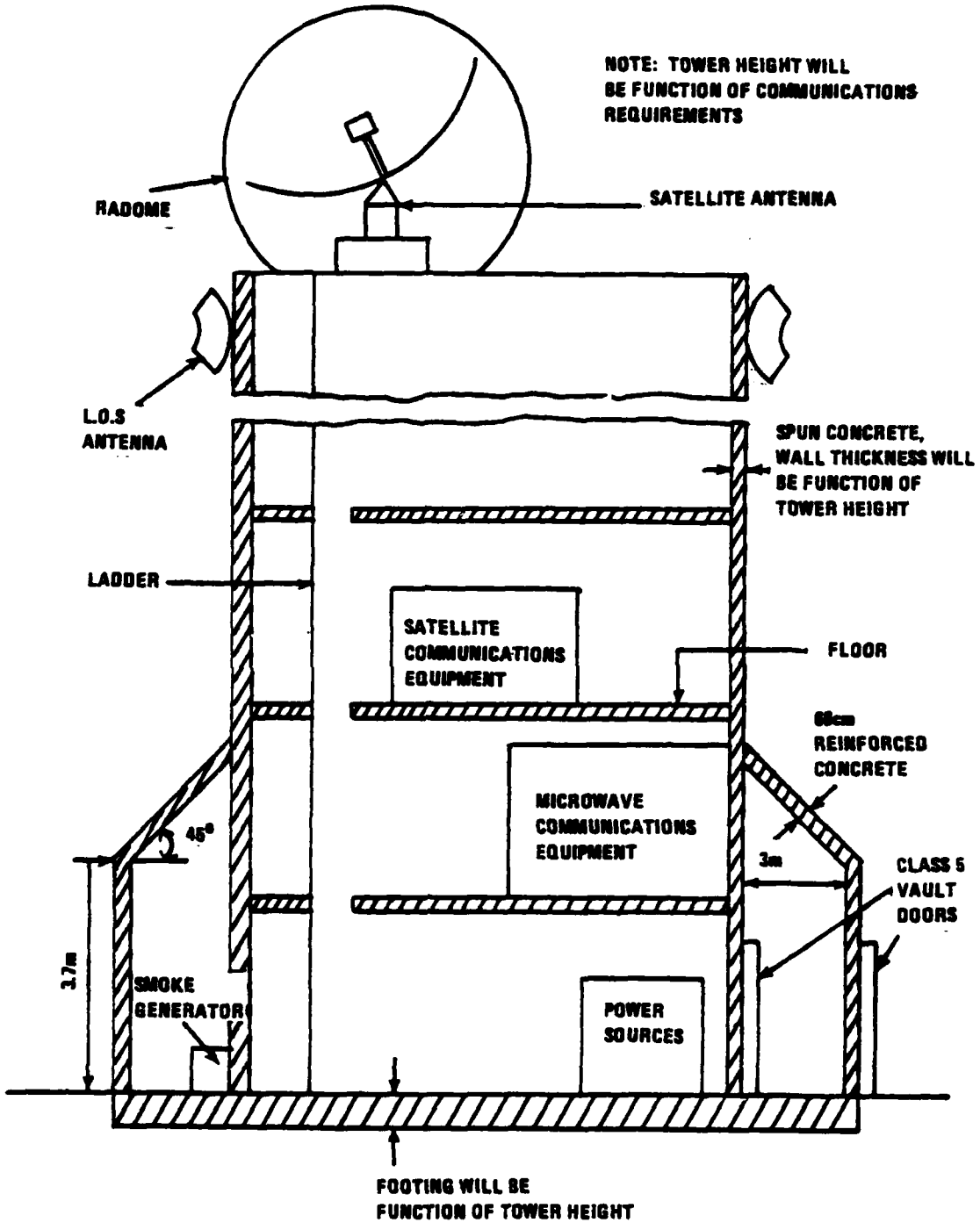


Figure b.

Figure 20. (Continued)

TOWER VAULTS

Description - All antenna towers and free standing antennas at unmanned DCS sites shall be housed in vaults.

Installation - Tower vaults shall be constructed in accordance with Figure a. Free standing antenna vaults shall be constructed in accordance with Figure a and shall be positioned in a way that will not interfere with the antennas operation.

Maintenance - Vaults shall be inspected periodically for damage or wear.

References - Barrier Technology Handbook Sandia Laboratories, Albuquerque, New Mexico, April 1978.

Construction Design Criteria for Physical Protection of Air Force Operated DCS Sites, U.S. Air Force, HQ AFCS/DEO, October 1979.

Figure 21. Tower Vaults

TOWER VAULTS (Continued)

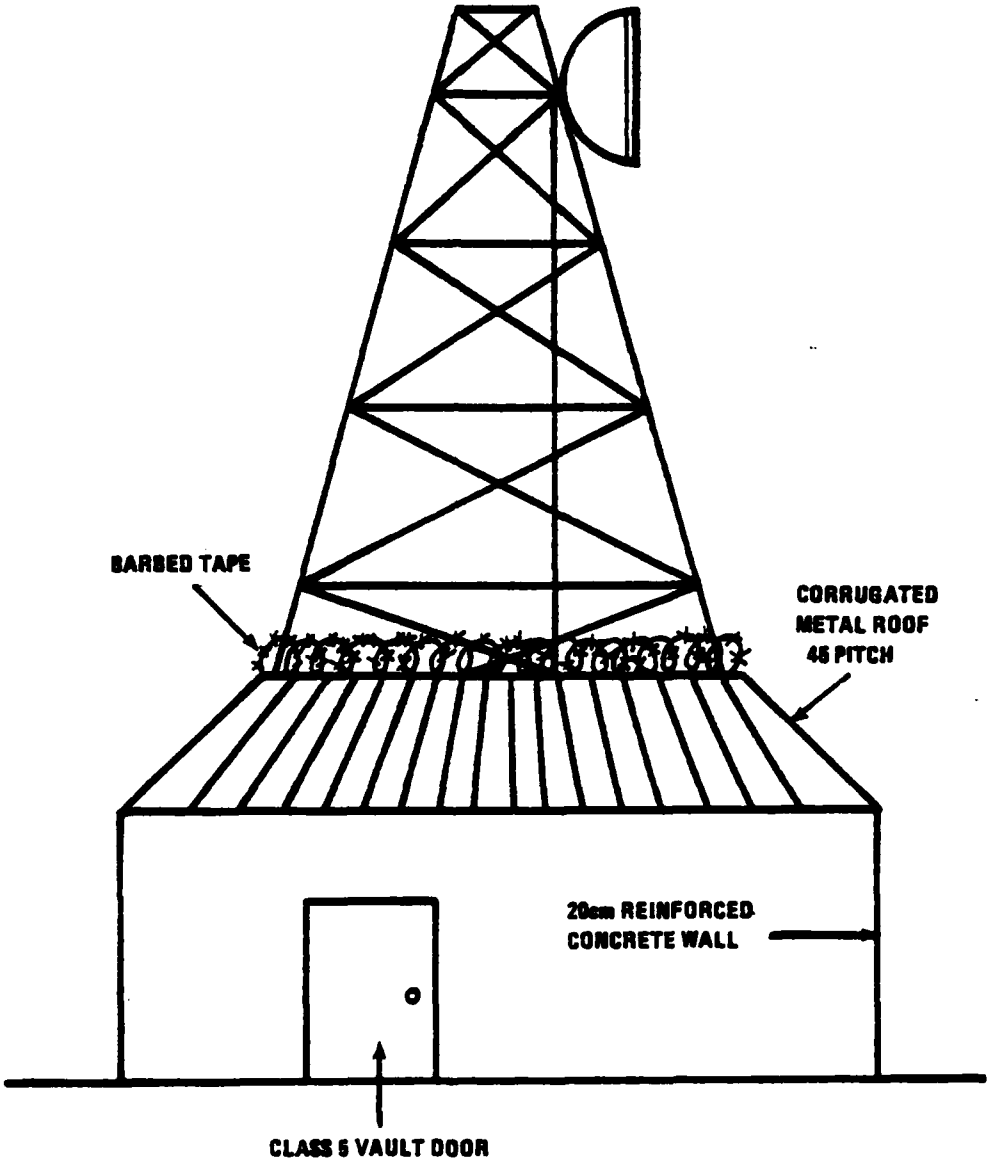


Figure a

Figure 21.(Continued)

SMOKE GENERATOR

Description - Smoke generators shall be installed to hinder intruder access to essential equipments.

Installation - Smoke generators shall be capable of filling the building or vault with smoke in less than one minute and maintaining the smoke level for 30 minutes.

Maintenance - Smoke generators shall be inspected periodically for degradation. In the advent of smoke generator activation, clean-up crews shall be dispatched as soon as possible to prevent corrosion of equipment.

References - AMCP 706-185, Engineering Handbook, Military Pyrotechnics Series, Part I, Theory and Application, U.S. Army Materiel Command.

Barrier Technology Handbook, Sandia Laboratories, Albuquerque, New Mexico, April 1978.

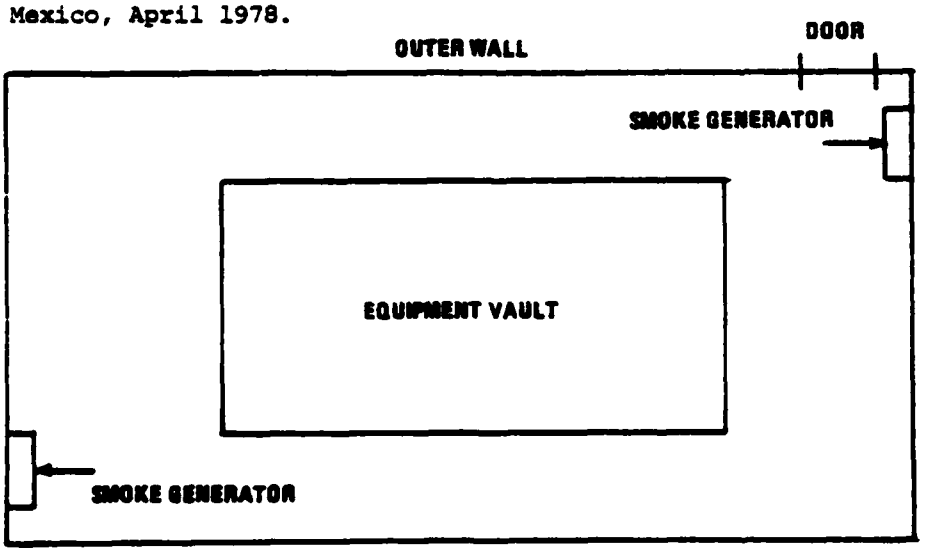


Figure 22. Smoke Generator

PERSONNEL DOORS

Description - All personnel doors at DCS sites shall be protected by armor plate and shall incorporate a minimum of 4 deadbolt locks.

Installation - All personnel doors at DCS sites shall be constructed in accordance with Figure a. Deadbolt locks shall be used in accordance with Figure b.

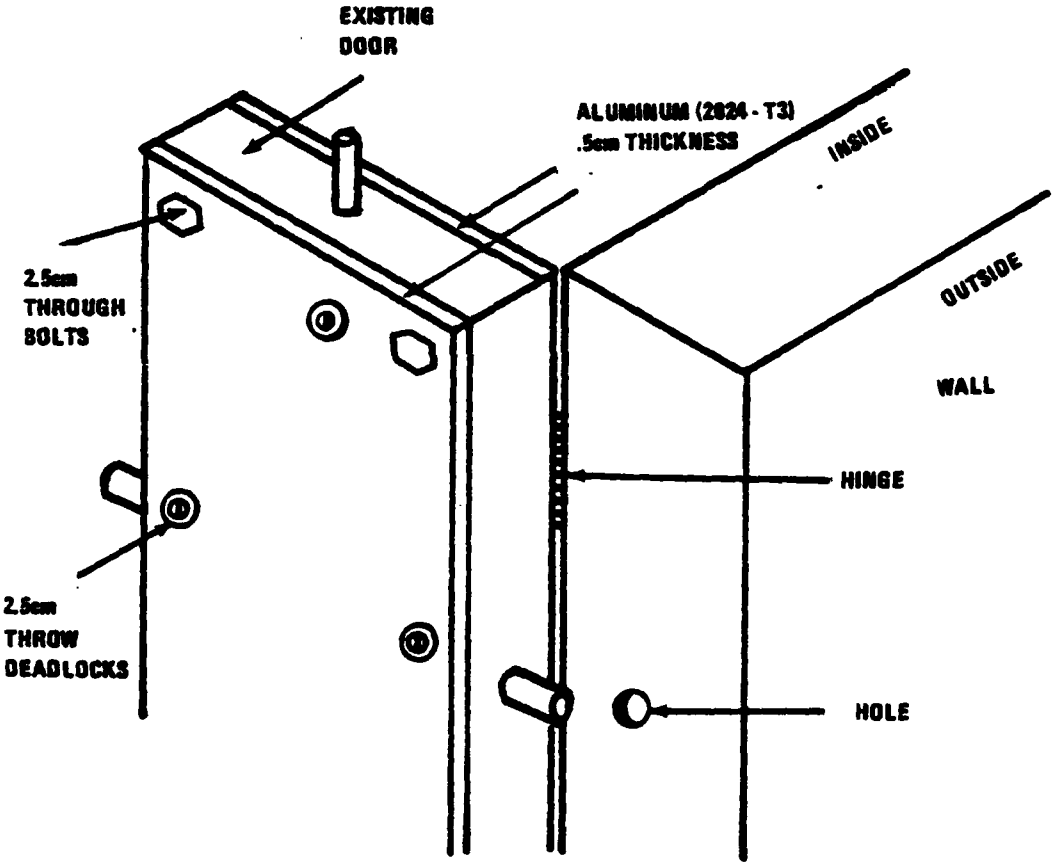
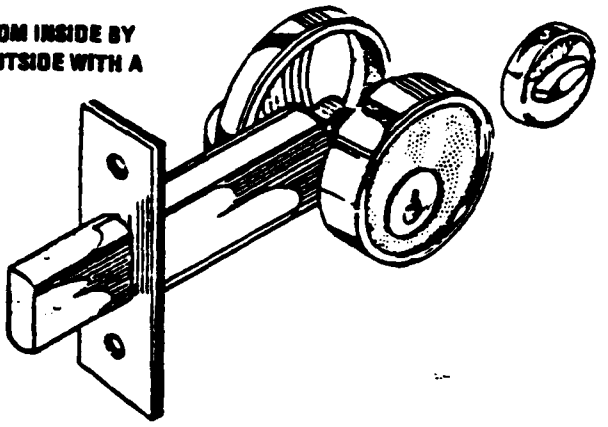


Figure a

Figure 23. Personnel Doors

PERSONNEL DOORS (Continued)

NOTE: BOLT MAY BE OPERATED FROM INSIDE BY THE THUMB TURN OR FROM THE OUTSIDE WITH A KEY.



2.5cm THROW DEADLOCK

Figure b

Maintenance - Personnel doors shall be inspected daily at manned DCS sites and upon every visit at unmanned sites. Doors shall be inspected for damage, wear and tampering and loosened bolts. If a door has been degraded, effectual repairs shall be made as soon as possible.

References - Physical Security, U.S. Army Field Manual 19-30, March 1979.

Barrier Technology Handbook, Sandia Laboratories, Albuquerque, New Mexico, April 1978.

Figure 23. (Continued)

WINDOW PROTECTION

Description - Armor plating shall be used to seal all windows and nonessential doors at DCS facilities.

Installation - All nonessential openings shall be sealed with armor plate in accordance with Figure a.

Maintenance - Armor plates shall be inspected daily at manned DCS sites and upon every visit to unmanned sites. Plates shall be inspected for tampering or loosened bolts.

References - Barrier Technology Handbook, Sandia Laboratories, Albuquerque, New Mexico, April 1978.

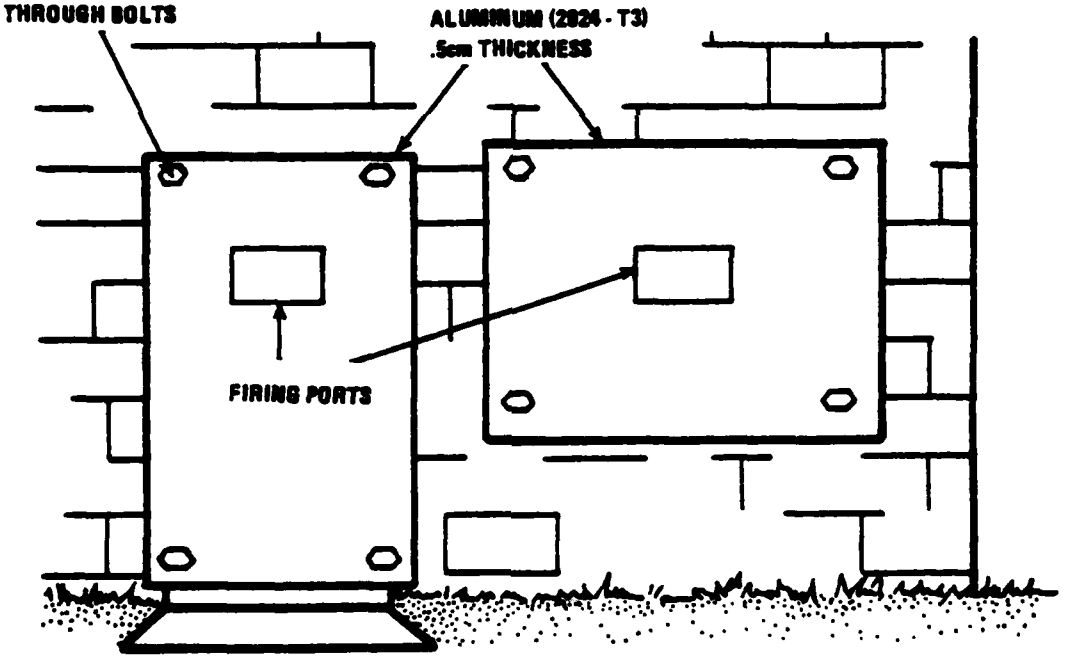


Figure a

Figure 24. Window Protection

DOOR SENSOR

Description - The door sensor shall consist of a balanced magnetic switch and actuating magnet mounted on the interior side of the door. When the door is opened the magnetic field at the switch location decreases, actuating the switch and producing an alarm condition.

Installation - The magnetic switch shall be mounted on the interior side of the door in accordance with Figure a. The gap between the

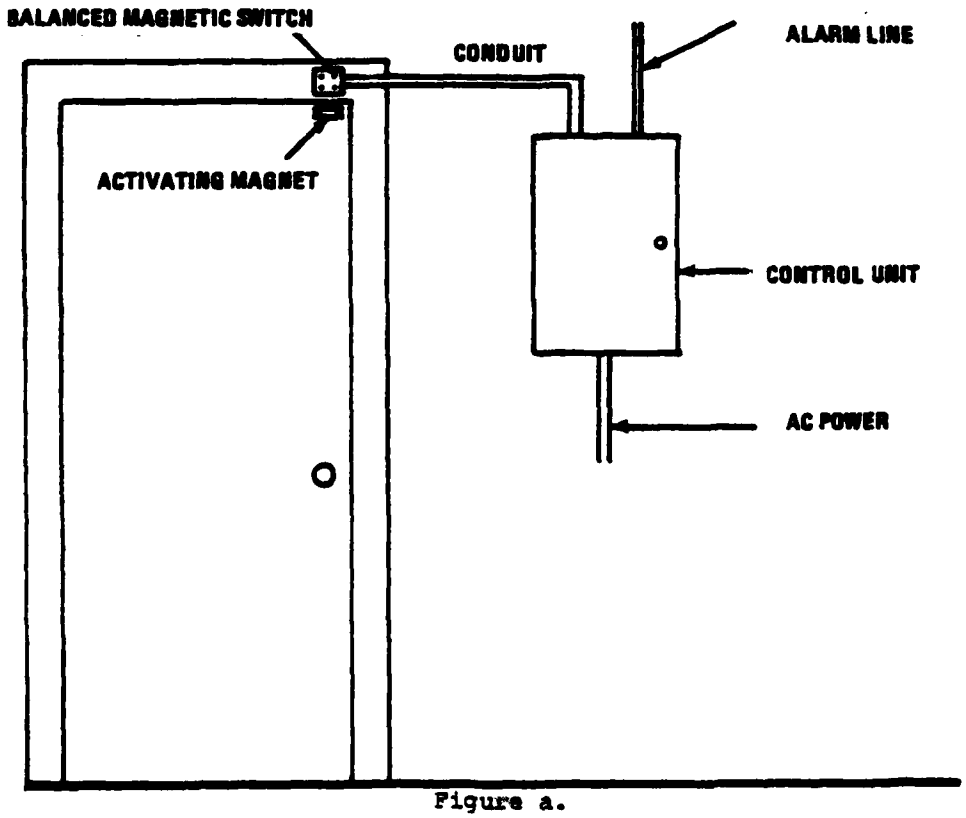


Figure a.

Figure 25. Door Sensor

DOOR SENSOR (Continued)

magnet and switch shall be as small as possible without interfering with door operation. Electrical wiring for the sensors and control unit shall be encased in steel conduit.

Maintenance - Periodic performance testing shall be conducted. If the sensor is suspected of degraded performance, testing shall be initiated.

References - Intrusion Detection Systems Handbook, Vol. I, Sandia Laboratories, Albuquerque, New Mexico, July, 1980.

Physical Security, U.S. Army Field Manual 19-30, March 1979.

Figure 25.(Continued)

MICROPHONE SENSORS

Description - Microphone sensors shall be located in equipment buildings and tower vaults at unmanned DCS sites to detect penetration attempts.

Installation - Microphone sensors shall be installed in accordance with Figure a. The microphone output shall be routed through an audio line to the facility responsible for sensor monitoring and alarm assessment.

Maintenance - Microphone sensors shall be tested periodically for degraded performance. Necessary repairs or replacements shall be made as soon as possible.

References - Physical Security, U.S. Army Field Manual 19-30, March 1979.

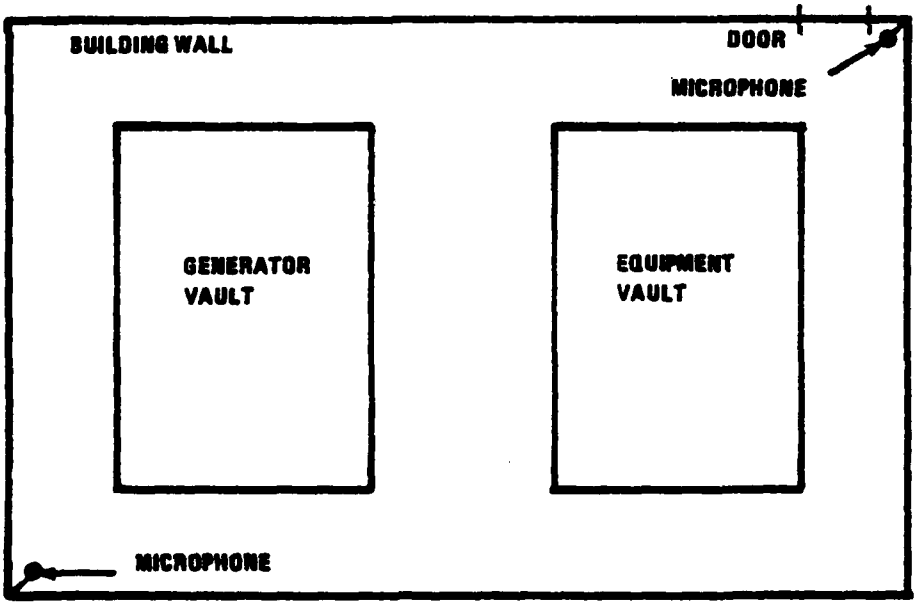


Figure a.

Figure 26. Microphone Sensors

RADOMES

Description - Radomes shall be installed on all antennas to prevent visual targeting of the antenna feedhorn by a standoff attacker.

Installation - Radome selection and installation shall be in accordance with military specification MIL-R-7705B. Typical radomes for a microwave relay antenna and a satellite terminal antenna are depicted in Figures a and b. Tower mounted radomes shall be dark in color.

Maintenance - Radomes shall be inspected periodically for degradation.

References - Department of Defense, General Specifications for Radomes, MIL-R-7705A (14 January 1975).

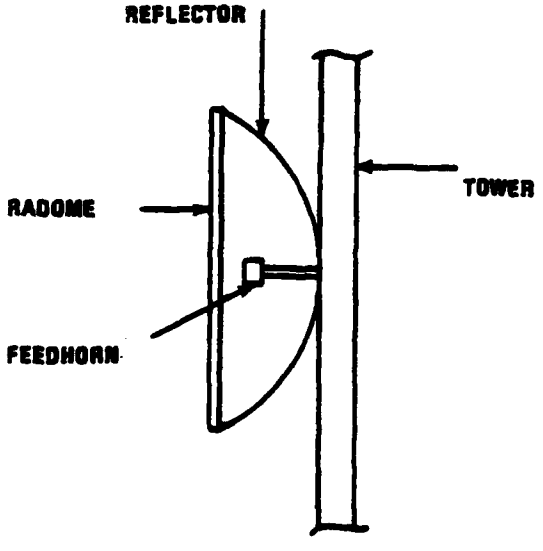


Figure a

Figure 27. Radomes

RADOMES (Continued)

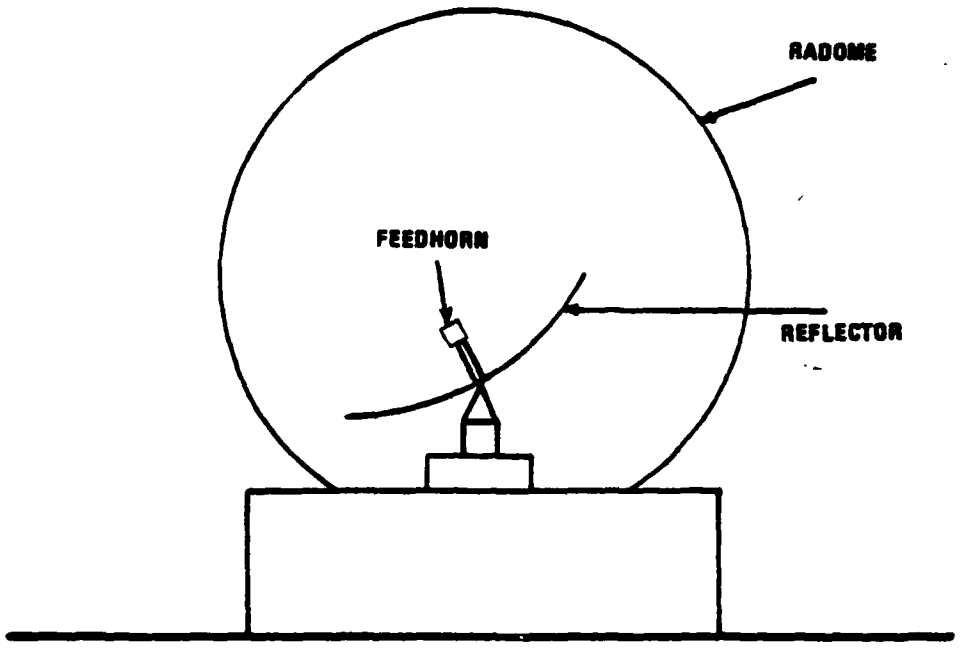


Figure b

Figure 27. (Continued)

WAVEGUIDE PROTECTION

Description - All waveguides shall be encased in a lightweight armor duct to prevent visual targeting by a standoff attacker and to protect against small arms fire.

Installation - Waveguide duct shall be constructed in accordance with Figure a.

Maintenance - Waveguide duct shall be inspected daily at manned DCS sites and upon every visit at unmanned sites.

References - Barrier Technology Handbook, Sandia Laboratories, Albuquerque, New Mexico, April 1978.

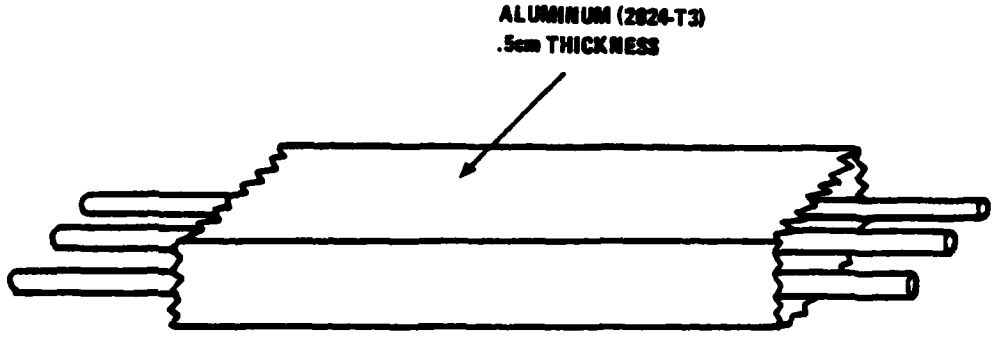


Figure a

Figure 28. Waveguide Protection

GUY WIRE PROTECTION

Description - Guy wires and guy wire anchors shall be protected at all DCS sites.

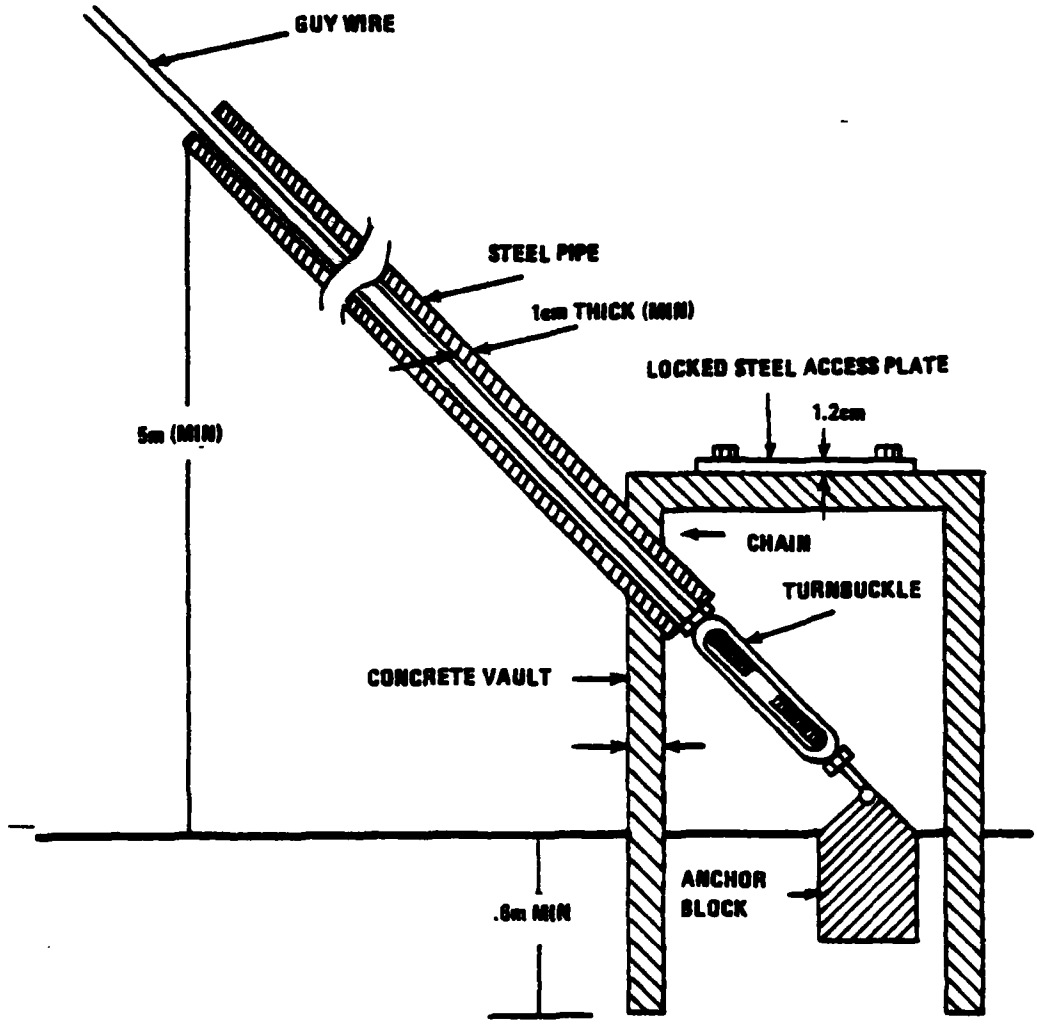


Figure a

Figure 29 Guy Wire Protection

GUY WIRE PROTECTION (Continued)

Installation - Metal guy wire pipe sleeves and concrete anchor vaults shall be installed in accordance with Figure a. Locks used shall be in accordance with pargraph 5.1.3.3.5.

Maintenance - The anchor vault shall be inspected periodically for damage wear, tampering, or loosened bolts. If an anchor vault has been damaged, effectual repairs shall be made as soon as possible.

References - Construction Design Criteria for Physical Protection of Air Force Operated DCS Sites, AF CS/DEO, U.S. Air Force, October 1979.

Figure 29 (Continued)

EQUIPMENT VAULT

Description - All essential communications equipment and power sources at unmanned DCS sites shall be housed in equipment vaults.

Installations - Equipment vaults shall be constructed in accordance with Figure a. Each vault shall have one door constructed in accordance with Figure b.

Maintenance - Equipment vaults shall be inspected periodically for damage or wear. Necessary repairs or replacements shall be made as soon as possible.

Reference - Barrier Technology Handbook, Sandia Laboratories, Albuquerque, New Mexico, April 1978.

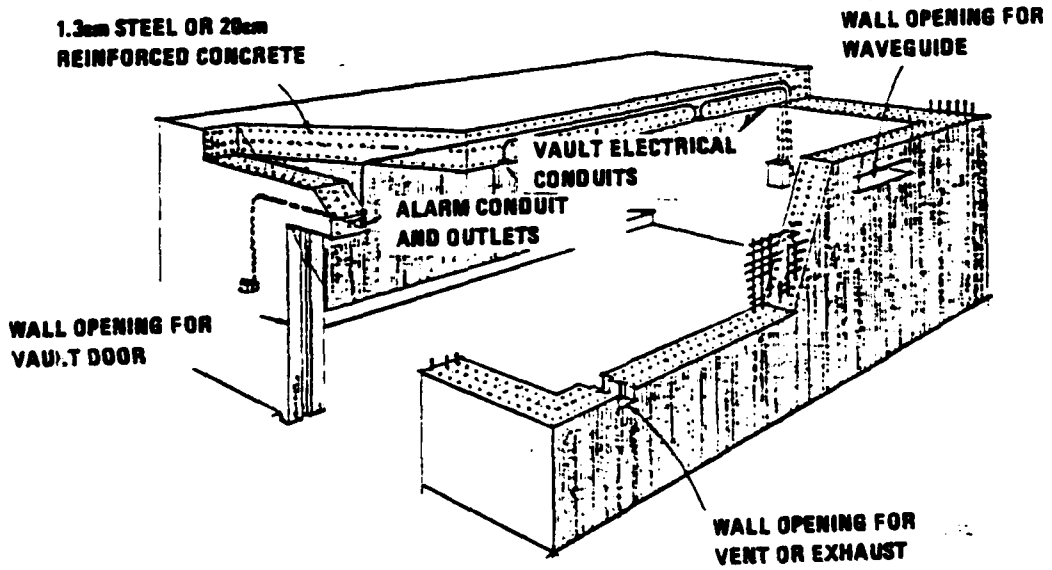


Figure a

Figure 30. Equipment Vault

EQUIPMENT VAULT (Continued)

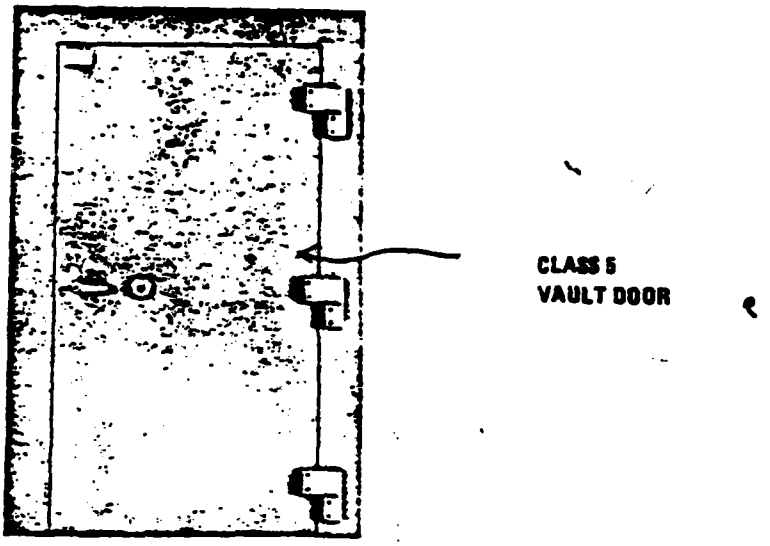


Figure b

Figure 30. (Continued)

TOWER LEG PROTECTION

Description - All tower supports shall be encased in protective sleeves.

Installation - Self-supporting tower legs shall be encased in sleeves that are constructed in accordance with Figure a.

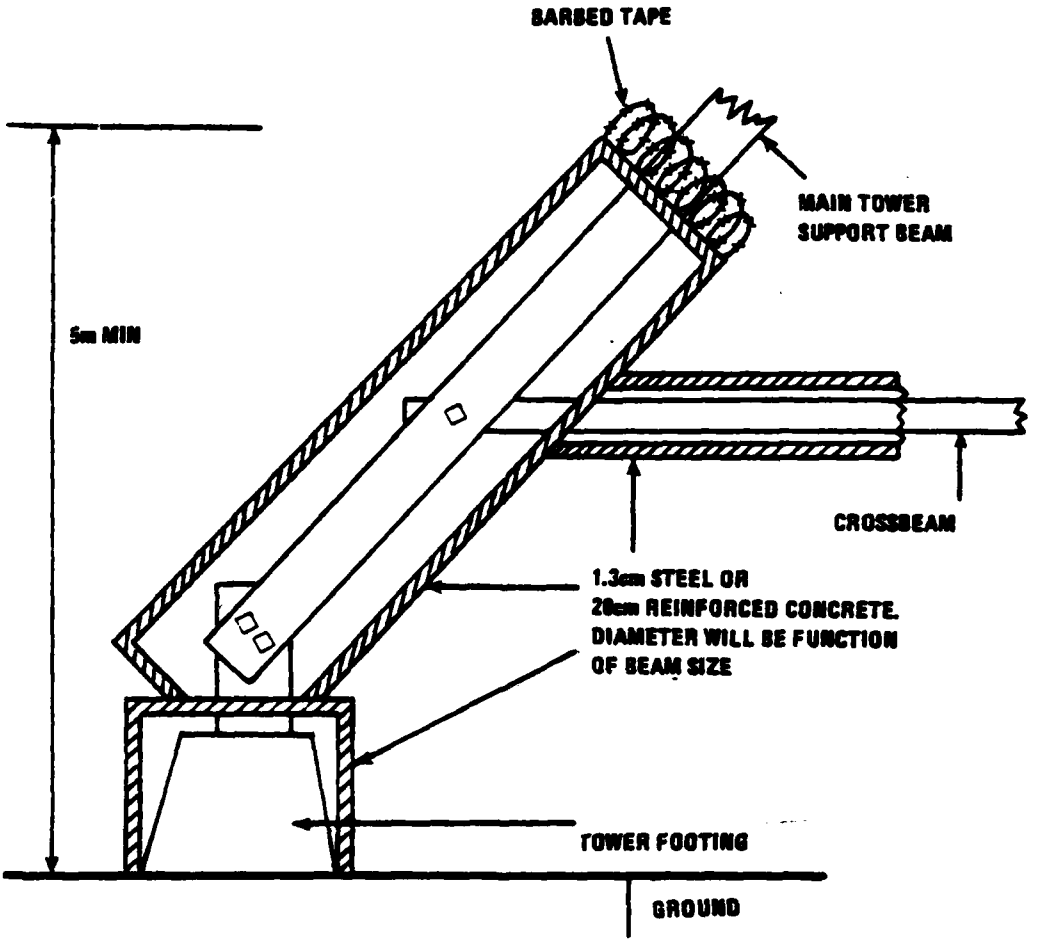


Figure a

Figure 31.Tower Leg Protection

TOWER LEG PROTECTION (Continued)

Guyed towers shall be encased in accordance with Figure b.

Maintenance - Tower leg sleeves shall be inspected periodically for wear and tampering.

References - Barrier Technology Handbook, Sandia Laboratories, Albuquerque, New Mexico, April 1978.

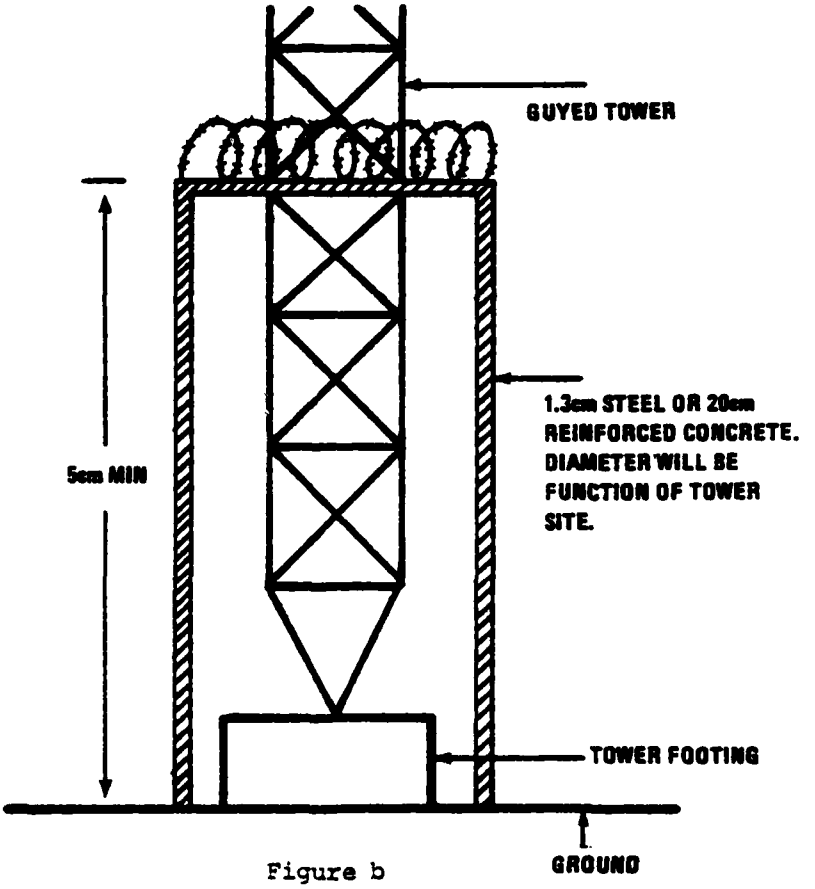


Figure b

Figure 31. (Continued)

PERSONNEL ENTRANCE VESTIBULE

Description - The vestibule shall be designed to allow the entry of a single person at a time. The doors shall be designed so that only one opens after the other is shut and locked.

Installation - The vestibules shall be installed at all main personnel control points to restrict and control access into buildings. The outer door may be operated by a key or cipher lock. It is preferable that the inner door be controlled by personnel inside the facility who could verify the identity of persons entering the vestibule.

The walls, doors and roof of the vestibule shall provide the same resistance to penetration as the exterior walls of the facility provide.

Figure 32.
Personnel Entrance Vestibule

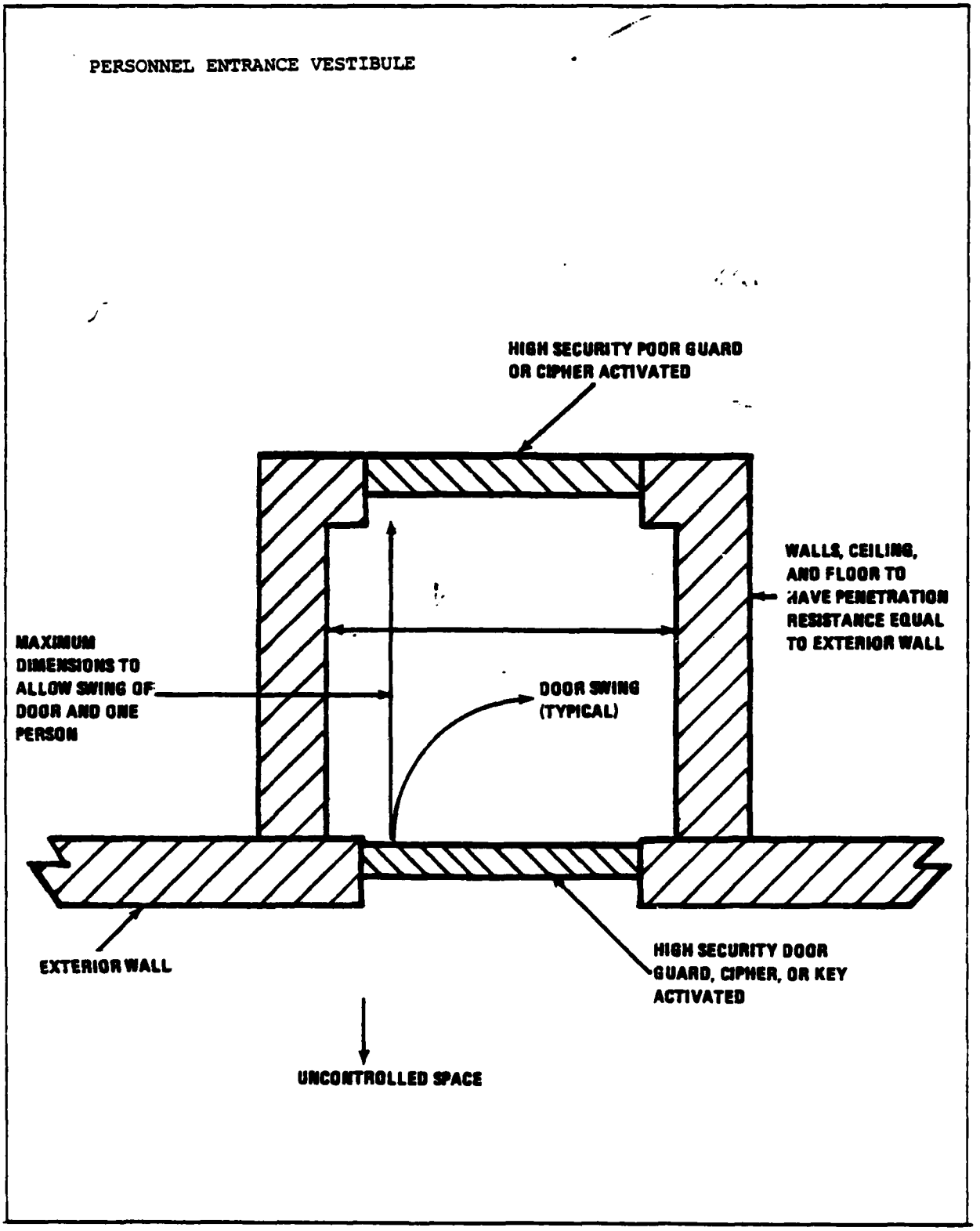


Figure 32. Personnel Entrance Vestibule
Top View

BLAST AND FRAGMENTATION
BUFFER CURTAIN

Description - The curtain shall be of high impact blast resistant material, e.g., 3/4 KEVLAR, to minimize possibility of damage by explosives and resulting wall fragments.

Instllation - The curtain shall be attached to a steel frame at least 12 inches from the exterior wall. The curtain shall be hung from top of exterior wall to floor. Space shall be provided at the top of the curtain to relieve overpressure created by the detonation of explosives.

Figure 33.
Blast and Fragmentation Buffer Curtain

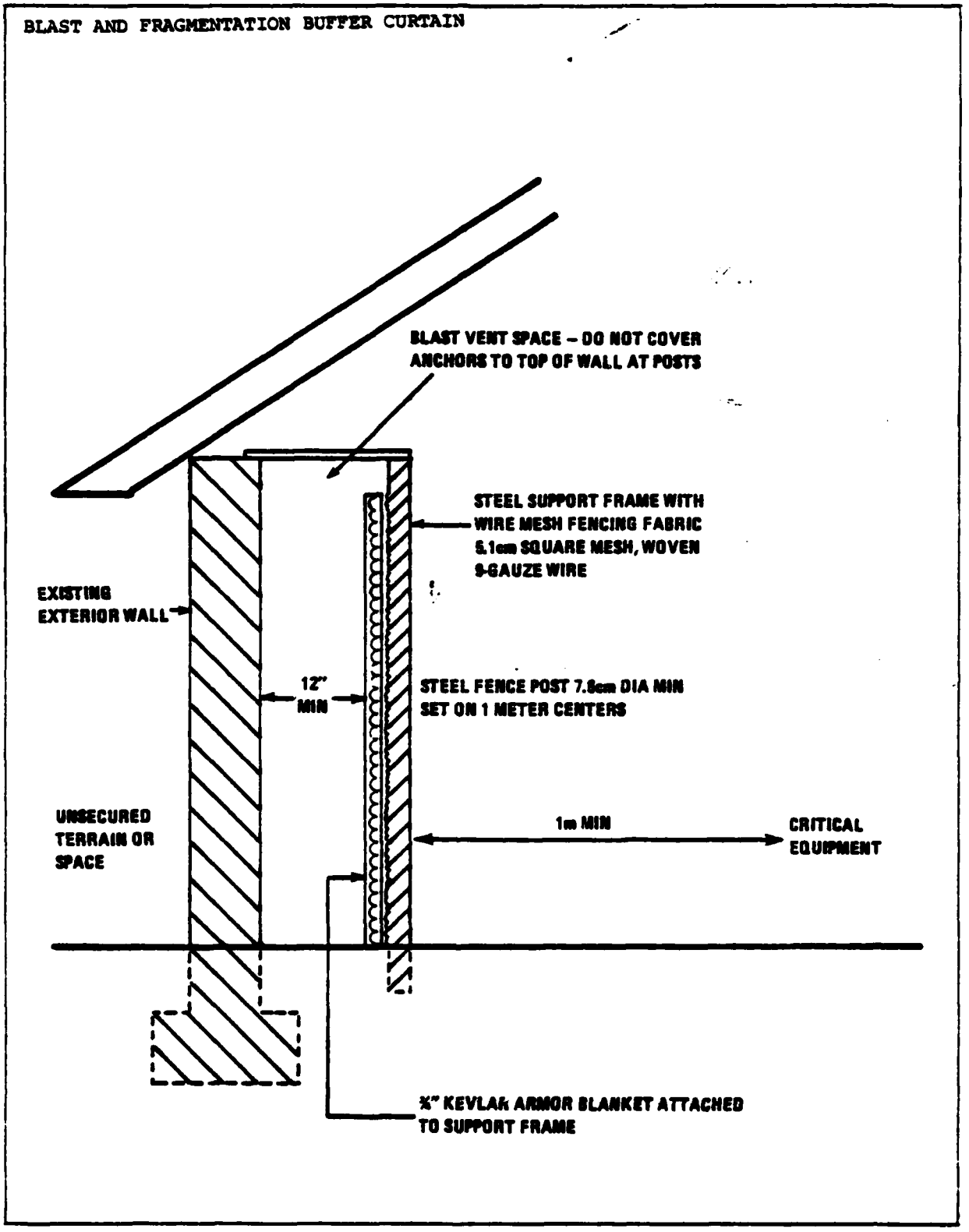


Figure 33. Blast and Fragmentation Buffer Curtain

APPENDIX A

Topical Outline for

Site Security Program Plan

1. Site Identification
2. Threat Analysis
   - 2.1 Threat Profile Based Upon Intelligence Agency Inputs
   - 2.2 History of Incidents at Site or Adjacent Sites
   - 2.3 Site Specific Threat Matrix
3. Site Susceptibility Analysis
   - 3.1 Site Functional Analysis and Failure Mode Description
   - 3.2 Site Survey and Description of Physical Layout
   - 3.3 Site Susceptibility Description
4. Threat-Vulnerability Matrix

   (Correlation of threat capabilities and site susceptibilities to identify specific site vulnerabilities)
5. Determination of Site Criticality and Endurability Requirements
   - 5.1 Mission Analysis
   - 5.2 Specific DCS Requirements
   - 5.3 Endurability Requirements for Site
6. Identification of Available Countermeasure Options for the Site
   - 6.1 Deterrence Measures
   - 6.2 Detection Measures
   - 6.3 Assessment Measures

6.4 Hardening Measures

6.5 Reaction Force Measures

7. Protection Allocation Matrix

(Correlation of site vulnerabilities with available countermeasure options)

8. Security Measures Effectiveness Analysis

8.1 Analysis of Aggregated Effectiveness of Physical Security Measures

8.2 Comparison of Aggregated Effectiveness with Site Endurability Requirements

8.3 Selection of Feasible Security Measures

9. Measures Implementation Plan

9.1 Schedule for Implementation

9.2 Task Assignments to Specific Agencies and Units

9.3 Procedures for Monitoring Implementation

9.3.1 Intrusion Detection and Assessment Testing Procedures

9.3.2 Human Activity Testing Procedures

10. On-Going Operations

10.1 Life-Cycle Operation and Maintenance of Physical Security Equipment

10.2 Memorandum of Understanding and Orders for Coordination and Delivery of Security Services by Security Agencies

10.3 Procedures for Regular Inspection

11. Budgeting and Programming

11.1 Determination of Funding Requirements by Year

11.1.1 Acquisition and Installation

11.1.2 Operations and Maintenance

11.2 Preparation and Submission of Funding Documents

11.3 Coordination of Security Program Requirements with Other Budget and Programming Processes

(CLASSIFICATION)

APPENDIX B

SECURITY PLAN OUTLINE

Name of Facility

Address, Location or Other Descriptive Data

1. Mission of the facility.

2. Purpose. (A brief statement of the purpose of the plan. In general, the intent is to ensure that good planning has integrated all available forces, devices and equipment into an effective security system.)

3. Objectives. (A brief statement of security objectives, e.g., preclude damage to a manned site, minimize damage to an unmanned site or ensure continued communications functions for a certain period of time after site penetration is initiated.)

4. Threat Analysis. (This requirement should be levied upon and be prepared by the appropriate military department counterintelligence/ investigative activity which is responsible for the geographical area of the military installation concerned. It would analyze the threat from terrorism, espionage, sabotage, theft, vandalism, etc., and would identify any known individuals or organizations which pose these threats. The threat analysis will be updated at least annually, or more frequently if warranted by changing conditions. Preparation of the analysis by the appropriate military department counterintelligence/investigative organization will insure strict compliance with the provisions of DoD Directive 5200.27 "Acquisition of Information Concerning Persons and

Organizations Not Affiliated with the Department of Defense," March 1, 1971, and military department implementing regulations.)

5. Vulnerability. (Define critical and other structures, buildings and work areas that require protection. Consider location, size, function and contents.)

6. Priorities. (Establish priorities for protecting various facilities within the site.)

7. Security Zones. (Define the areas and boundaries of the security zones.)

8. Equipment and Devices to Detect Intruders and to Delay Intrusion or Damage to Site Facilities.

a. Zone 0.

(1) Clear zone.

(a) Width

(b) Surface undulations and ditches

(c) Obstacles (i.e., poles, trees, boulders, structures, etc.) that can not be removed

(d) Culverts, utility tunnels and other structures

(2) Access Road

(a) Road side vehicle barriers

(b) Entrance control gate, locking means and procedures

(c) Speed control barrier

(d) Access road sensor system, assessment and response

(3) Parking lot

(a) Vehicle barriers

(4) Utility lines

(a) Commercial power

(b) Communications

(c) Sensors

b. Zone 1

(1) Perimeter fence

(a) Type and construction

(2) Gates

(a) Type and construction

(b) Locking means and procedures

(c) Entry control and procedures

(d) Emergency entry procedures

(3) Warning signs

(a) Specifications

(b) Location

(4) Clear zone

(a) Width

(b) Surface undulations and ditches

(c) Culverts, utility tunnels and other structures

(5) Sensors

(a) Type and location

(b) Alarm annunciation

(c) Alarm assessment and response

c. Zone 2

(1) Inner fence

(a) Type and construction

(2) Sensors on inner fence

(a) Type and location

(b) Alarm annunciation

(c) Alarm assessment and response

(3) Gates

(a) Type and construction

(b) Locking means and procedures

(c) Entry control and procedures

(d) Emergency entry procedures

(4) Gate guard (manned sites)

(a) Location (gatehouse)

(b) Duties and procedures

(5) Security lighting

(a) For perimeter, gates, interior areas and structures

(b) Type (area, glare, controlled) and source

(c) Location, orientation and strength

(d) Use and control

(6) Closed circuit television (CCTV) (manned sites)

(a) Camera type and locations

(b) Monitor location and responsibilities

(c) Alarm assessment procedures

(d) Intrusion response procedures

(7) Guard tower (manned site)

(a) Type and location

(b) Communications equipment

(c) Alarm annunciation equipment

(d) Guard procedures

(8) Patrols

(a) Composition and equipment

(b) Frequency and time

(c) Mission(s)

d. Zone 3

(1) Building hardening

(a) Windows, doors, openings

(b) Entry control

(c) Door sensors and procedures (unmanned sites)

(d) Acoustic sensors and procedures (unmanned sites)

(e) Key control

(f) Weapons control (manned sites)

(g) Smoke generation (unmanned sites)

(2) Antenna tower vaults (unmanned facilities)

(a) Configuration and construction

(b) Entry control

(c) Door sensors and procedures

(d) Acoustic sensors and procedures

(e) Smoke generation

(3) Antenna tower barriers (manned sites)

(a) Type and construction

(b) Locking means and procedures

(c) Entry control

(4) Other

(a) Radomes

(b) Waveguide protection

(5) Guy wire protection

(a) Anchor vault

(b) Guy wire sleeve

(c) If outside the inner fence, secure as separate unmanned site.

e. Zone 4

(1) Equipment vaults (unmanned sites)

(a) Type and construction

(b) Locking means and procedures

(c) Entry control

(2) Tower leg protection

(a) Sleeve type and construction

(3) Guy wire anchor vaults

(a) Sleeve type and construction

9. Inspection and Maintenance

a. Responsibility and frequency

b. Required items

c. Maintenance responsibilities

10. Power Failure

    a. Emergency generator

    b. Required lighting

    c. Intrusion detection systems

    d. Alarm assessment

11. Response forces

    a. On-site (manned sites)

        (1) Designation of personnel

        (2) Organization

        (3) Authority and jurisdiction

        (4) Weapons and equipment

        (5) Use of deadly force

        (6) Training

        (7) Actions in adverse weather

        (8) Posts

            (a) Location and area of responsibility

            (b) Duties and reporting procedures

    b. Off-site

        (1) Purpose and mission

        (2) Size, composition and organization

        (3) Personnel designation and location

        (4) Weapons and equipment location

        (5) Designation and protection of vehicles

        (6) Training

        (7) Testing

12. Emergency Actions

    a. Natural or man-made disaster

    b. Medical emergency

13. Coordination

    a. Supporting forces

    b. Nearby units and cognizant civil authorities

APPENDIX C

Security Planning Checklist

for

Defense Communications System Sites

PART I. Land/Space/Planning Requirements

1. Can the site be located within or adjacent to an existing military installation? (new sites)
2. Has the site locality been surveyed to identify EMR problems? (new sites)
3. Do land requirements include provision for easement or ownership as necessary? (new sites)
4. Has an environmental impact statement been prepared? (new sites)
5. Have security considerations been given appropriate priority in the plan and site layout? (new sites)
6. Do planning and programming include adequate resources for both installation and operation of the site security system? (Consider O&M, staffing, logistics and training.)

PART II. Vulnerability

1. Has the threat been assessed?
2. Have the site mission and the threat been analyzed to determine the required level of protection?

3. Has a site hardening analysis been performed to determine the most cost-effective method of achieving the required level of protection?

4. Are contingency plans realistic?

PART III. Security Planning

1. Are trained security personnel participating in security planning?

2. Have the objectives of the security program been clearly identified and considered?

3. Has an appropriate detailed security plan been prepared?

4. Is the security-in-depth concept maintained?

5. Have selection and application of security equipment ensured that the best combination is employed in relation to the problem?

6. Do clear zones, lighting, barriers, intrusion detection alarms, assessment and delay systems accomplish the designed purposes?

7. Are security communications systems adequate?

8. Are response force facilities and plans realistic and adequate to accomplish the security mission?

9. Are response force weapons and equipment properly secured yet easily available?

10. Do plans ensure appropriate training, exercises and tests for response forces?

11. Do plans ensure adequate tests to ascertain that detections systems were a) installed correctly and b) operating each day?

12. Are provisions made for emergency power for security systems?


FILMED
8